УТВЕРЖДЕН
ПФНА.501540.001 РЭ-ЛУ

ШЛЮЗ БЕЗОПАСНОСТИ

WAF Dallas Lock

(версия 1.15.22)

Руководство по эксплуатации

ПФНА.501540.001 РЭ

Листов 120

АННОТАЦИЯ

Данное руководство по эксплуатации освещает вопросы настройки и сопровождения **Шлюза безопасности Web Application Firewall Dallas Lock** и предназначено для администраторов, ответственных за эксплуатацию системы защиты информации.

В документе представлены элементы графических интерфейсов, которые соответствуют эксплуатации **Шлюза безопасности Web Application Firewall Dallas Lock**.

Вы можете посетить сайт компании-разработчика (ООО «Конфидент») www.confident.ru или сайт продуктовой линейки www.dallaslock.ru.

На сайте продукта можно получить информацию о **Шлюзе безопасности Web Application Firewall Dallas Lock**, предыдущих версиях продукта, а также заказать комплекс услуг по проектированию, внедрению и сопровождению. Также при необходимости можно обратиться в службу технической поддержки по электронному адресу: helpdesk@confident.spb.ru.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Данное руководство предназначено для администраторов Шлюза безопасности Web Application Firewall Dallas Lock (далее по тексту — **WAF Dallas Lock**), осуществляющих первоначальную настройку приложения и его администрирование.

Руководство рассчитано на наличие у администратора **WAF Dallas Lock**:

- знаний об информационной безопасности и основах построения защищенных корпоративных систем;
- знаний в области веб-технологий;
- знаний в области работы веб-серверов, сетевого администрирования;
- навыков работы с межсетевыми экранами.

WAF Dallas Lock представляет собой программный комплекс, поставляемый на компакт-диске в виде ISO-образа с первоначальной конфигурацией, который инсталлируется на физическое устройство. Виртуальные машины **WAF Dallas Lock** разворачиваются в выделенной виртуальной инфраструктуре клиента в средах VMware, Hyper-V, VirtualBox.

Руководство состоит из 6 глав и имеет следующую структуру:

1. Глава 1 содержит общее описание назначения и возможностей **WAF Dallas Lock**.
2. В Главе 2 описан алгоритм развертывания **WAF Dallas Lock** от первого запуска до внедрения в сеть и работы в штатном режиме с первоначальными настройками.
3. Главы 3–6 подробно описывают функциональные возможности основных подсистем, модулей, механизмов и настроек **WAF Dallas Lock**.

ТЕРМИНЫ И СОКРАЩЕНИЯ

Сокращение	Полная формулировка
БРП	База решающих правил
ДБ	Домен безопасности
ЕЦУ	Единый центр управления Dallas Lock
КЦ	Контроль целостности
МЭ	Межсетевой экран
СОВ	Система обнаружения вторжений
УЦ	Удостоверяющий центр
CMS	Content Management System, система управления сайтом
DL	Dallas Lock
DMZ	Demilitarized Zone, демилитаризованная зона
LAN	Local Area Network, локальная вычислительная сеть
UTM	Unified threat management, универсальное устройство, обеспечивающее комплексную защиту от сетевых угроз
WAN	Wide Area Network, глобальная компьютерная сеть
WAF	Web Application Firewall, межсетевой экран для защиты веб-приложений

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение и возможности

WAF Dallas Lock является межсетевым экраном прикладного уровня со вспомогательными подсистемами межсетевого экранирования и обнаружения вторжений.

WAF Dallas Lock обладает следующими основными возможностями:

- реализация защиты от угроз из списка OWASP TOP 10;
- анализ трафика веб-приложений и обнаружение атак (вторжений);
- блокирование попыток сетевых атак при работе с веб-приложениями;
- анализ поведения и обнаружение подозрительной активности пользователей веб-приложений;
- фильтрация сетевого трафика. Реализация фильтрации сетевого трафика по заданным правилам, возможность настройки правил и политик фильтрации;
- защита файлов cookie. Реализация защиты передачи файлов cookie от несанкционированного раскрытия и нарушения целостности;
- интеграция с Единым центром управления **Dallas Lock**;
- интеграция в SIEM-систему по протоколу syslog в формате leef.

1.2 Принципы функционирования

WAF Dallas Lock нацелен на защиту веб-серверов, расположенных в демилитаризованной зоне (DMZ), и сетевой инфраструктуры (LAN) от угроз, исходящих из глобальной сети Интернет (WAN) (см. Рисунок 1).

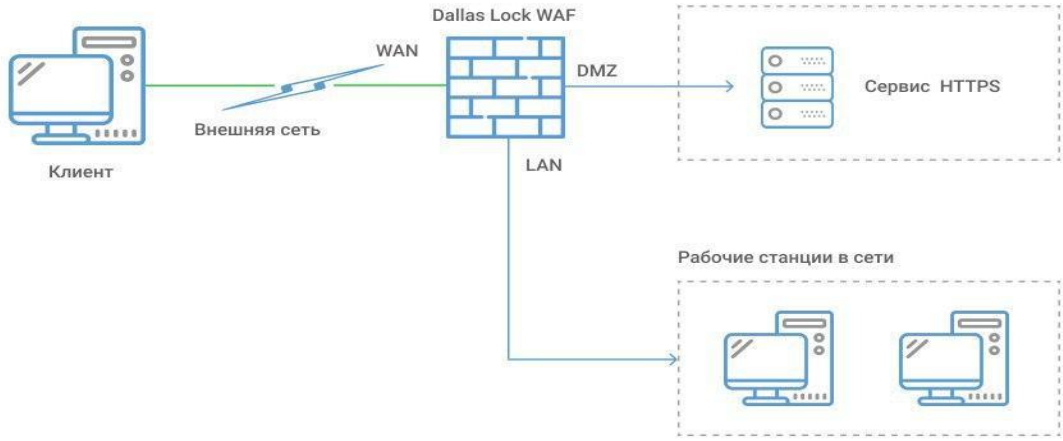


Рисунок 1. Типовая схема использования WAF Dallas Lock

Для удобства фильтрации и контроля трафика сетевые интерфейсы **WAF Dallas Lock** отнесены к различным «зонам» (LAN, WAN, DMZ), за каждой из которых закреплен соответствующий профиль межсетевого экрана. Межсетевое экранирование, обнаружение вторжений и защита веб-серверов реализуются заданием и своевременным обновлением администратором правил фильтрации и баз сигнатур атак.

В целях обеспечения надежности в **WAF Dallas Lock** предусмотрена подсистема контроля целостности и восстановления. Проверка целостности происходит периодически и по запросу администратора. В случае нарушения целостности **WAF Dallas Lock** переходит в аварийный режим. После ручного восстановления функционирование **WAF Dallas Lock** продолжается в штатном режиме.

Настройка **WAF Dallas Lock** осуществляется посредством веб-конфигуратора, разделенного на страницы, позволяющие задать новые значения параметров функционирования. Предусмотрена выгрузка настроек в виде архива конфигурационных файлов для хранения и восстановления работы **WAF Dallas Lock**.

1.3 Роли пользователей

Разграничение доступа к средствам администрирования осуществляется на основе системы ролей: администратор (root), аудитор (auditor) и внутренний пользователь (subadmin). Относительно каждой роли указываются доступные страницы настройки.

Администратор (root) — пользователь, наделенный всеми полномочиями на администрирование системы защиты. Подробнее об этой роли в пунктах 5.4.2 Настройки интерфейса управления WAF Dallas Lock и 5.5 Настройка пользователей.

Аудитор (auditor) — пользователь, наделенный правами на просмотр аудита и журналов системы защиты. Подробнее об этой роли в пункте

> Обратите внимание, что при сохранении настроек вы можете потерять доступ к управлению.

5.4.3 Параметры аудитора.

Внутренний пользователь (subadmin) — пользователь, имеющий доступ только к консольной оболочке WAF. Может выполнять конкретные команды, описанные в пункте 5.4.2.1 Базовые настройки.

1.4 Структура и составные модули

Меню управления **WAF Dallas Lock** расположено в верхней части страницы (см. Рисунок 2).

1. Основное меню с набором вкладок.
2. Имя хоста.
3. Иконки:
   - права администрирования;
   - общее количество сохраненных, но не принятых конфигурационных изменений WAF Dallas Lock (иконка не отображается, если все изменения были приняты);
   - состояние автоматического обновления WAF Dallas Lock;
   - иконка регистрации **WAF Dallas Lock** в домене безопасности Единого центра управления (иконка не отображается, если не зарегистрирован в домене безопасности);
   - переключение между светлой и темной темой графического интерфейса **WAF Dallas Lock**.

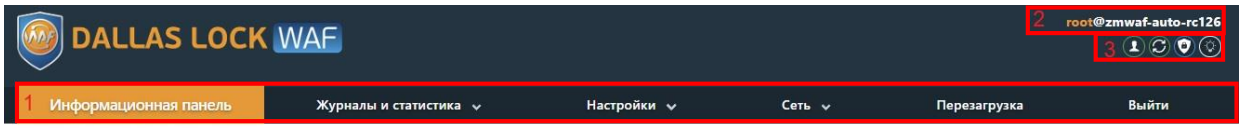


Рисунок 2. Меню управления WAF Dallas Lock

Меню шлюза безопасности **WAF Dallas Lock** состоит из следующих вкладок:

1. **Информационная панель.** Представляет собой набор виджетов и блоков статистических данных.

Включает в себя:

- **Атакуемые ресурсы.** Виджет с кольцевой диаграммой отображает статистику атак на веб-приложения из списка защищаемых **WAF Dallas Lock**.
- **Аппаратное обеспечение.** Мониторинг нагрузки на процессор, свободного объема оперативной памяти и места на устройстве для постоянного хранения информации, а также средней загрузки системы в режиме реального времени.
- **Все зафиксированные атаки.** Виджет с кольцевой диаграммой, на которой отображены девять наиболее массовых (по количеству) атак, обнаруженных **WAF Dallas Lock**, на все защищаемые ресурсы.
- **Источники атак**. Виджет с кольцевой диаграммой, на которой отображены источники всех зафиксированных атак.
- **Атаки, зафиксированные на ресурсы**. Ресурсы, по которым выводятся атаки, либо указываются вручную при помощи кнопки **Изменить ресурсы**, либо кликом левой кнопкой мыши по имени ресурса на виджете **Атакуемые ресурсы**.

- **Источники атак, зафиксированные на ресурсы.** Виджет содержит кольцевую диаграмму с источниками, с которых были зафиксированы атаки на наблюдаемые ресурсы (ресурсы, которые были добавлены в виджет **Атаки, зафиксированные на ресурсы**).
- **Уровни тревоги атак.** В данном виджете, на основании анализа зафиксированных атак, проводимого в режиме реального времени при получении новых данных, отображенных на кольцевой диаграмме атак, строится график уровней тревоги зафиксированных атак за выбранный период. Вертикальная ось обозначает количество зафиксированных атак, где максимальное число на оси равно максимальному количеству атак, отображаемых за период. Горизонтальная ось — ось времени, сегментированная на количество частей, в зависимости от выбранного периода времени, цена деления которой зависит от результата выборки на виджете **Все зафиксированные атаки**.
- **Уровни тревоги атак, зафиксированные на ресурсы**. В данном виджете, на основании анализа зафиксированных атак на ресурсы, проводимого в режиме реального времени при получении новых данных, отображенных на кольцевой диаграмме атак, строится график уровней тревоги зафиксированных на ресурсы атак за выбранный период. Вертикальная ось обозначает количество зафиксированных атак на ресурсы, где максимальное число на оси равно максимальному количеству атак на ресурсы, отображаемых за период. Горизонтальная ось — ось времени, сегментированная на количество частей, в зависимости от выбранного периода времени, цена деления которой зависит от результата выборки на виджете **Атаки, зафиксированные на ресурсы**.
- **Список инцидентов**. Блок список инцидентов содержит в себе зафиксированные данные по инцидентам безопасности, относящимся только к событиям МЭ Типа Г, а также инструментарий для поиска и сортировки этих данных.
- **Трафик в реальном времени.** График входящего и исходящего трафика реализован по интерфейсам в реальном времени.
- **Запросы в реальном времени.** График запросов в секунду в реальном времени.

Источником данных для графиков **Источники атак, зафиксированные на ресурсы** и **Уровни тревог атак, зафиксированные на ресурсы** являются ресурсы, выбранные на виджете **Атаки, зафиксированные на ресурсы** или перечень из пяти наиболее загруженных ресурсов.

2. Журналы и статистика. Подсистема учета и регистрации событий в **WAF Dallas Lock.**
Включает в себя:

- **Журналы аудита**. Вкладка содержит следующие журналы:
  - *Инциденты*. Журнал *Инциденты* содержит данные по инцидентам безопасности, зафиксированным **WAF Dallas Lock**.
  - *WAF*. Журнал *WAF* содержит события, основанные на сигнатурном анализе правил для межсетевого экрана уровня приложений.
  - *СОВ*. Журнал *СОВ* содержит события, связанные с подозрительной (опасной) активностью сетевых приложений (в т.ч. веб-ресурсов) и пользователей, которые основываются на сигнатурном и эвристическом методах анализа сетевого трафика, проходящего через **WAF Dallas Lock**.
  - *МЭ*. Журнал *МЭ* содержит события, основанные на сетевом трафике для межсетевого экрана уровня границы сети.
  - *Сетевые пакеты.* Журнал *Сетевые пакеты* содержит события, связанные с передачей пакетов данных по всем протоколам.
  - *Политики*. Журнал *Политики* содержит данные о модификации политик безопасности **WAF Dallas Lock**. Также содержит данные о создании, модификации и удалении учетных записей **WAF Dallas Lock**.
  - *Авторизация***.** Журнал *Авторизация* содержит информацию о попытках (удачных или неудачных) входа пользователей в графический интерфейс и консоль **WAF Dallas Lock**.
  - *Системный***.** Журнал *Системный*, содержит события **WAF Dallas Lock**, в том числе системные сообщения, сообщения процессов и сообщения планировщика заданий.
  - *Прокси***.** Журнал *Прокси* содержит события по регистрации HTTP-запросов к веб-приложению.

Возможна выгрузка выбранного журнала путем нажатия кнопки **Скачать**. Факт выгрузки журнала фиксируется в системном журнале.

- **Журнал ядра.** Содержит данные о системе.
- **Журнал аварийного режима**. Аварийный журнал содержит данные об истории команд, выполненных уполномоченным пользователем в аварийном режиме. Во вкладке *Текущий* представлен журнал команд после последней деактивации аварийного режима. Во вкладке *Предыдущий* представлен журнал команд до последней деактивации аварийного режима.
- **Сеть.** Содержит данные сетевой статистики.
  - *Сетевая статистика* — содержит список сетевых подключений по протоколам UDP и TCP.
  - *Состояние межсетевого экрана* — представлены таблицы IPTABLES (Filter, NAT, Mangle, Raw).
  - *Маршруты* — представлены правила маршрутизации.
- **Графики в реальном времени**. Страница содержит следующие графики:
  - *Загрузка системы* — на графике отображена динамика нагрузки системы в реальном времени интервалом за 1 минуту, 5 минут и 15 минут.
  - *Трафик в реальном времени* — отображение информации о входящем и исходящем сетевом трафике в реальном времени.
  - *Соединения* — отображение активных соединений в реальном времени по протоколам TCP, UDP и др.
- **Процессы.** Страница содержит текущее состояние работающих процессов. В таблице представлены в реальном времени:
  - идентификатор процесса;
  - имя пользователя, от которого запущен процесс;
  - текущий приоритет процесса;
  - приоритет процесса, выставленный командой nice (от -20 (наивысший) до 19);
  - полный объем виртуальной памяти, которую занимает процесс;
  - текущее использование оперативной памяти в реальном времени;
  - процент использования центрального процессора данным процессом;
  - процент использования оперативной памяти данным процессом;
  - время использования процессора в секундах;
  - текущее состояние процесса (S — спящий, R — запущен, Z — зомби);
  - команда, запустившая процесс;
  - кнопки **Завершить процесс** и **Принудительно завершить процесс.**
- **Сведения о системе**. Данная страница показывает общие данные о системе **WAF Dallas Lock**, в том числе значения контрольных сумм исполняемых файлов **WAF Dallas Lock**.

3. **Настройки.** Подсистема тонкой настройки межсетевого экрана. Включает в себя следующие функциональные модули:
   - **WAF.** Представляет собой межсетевой экран уровня веб-сервера. Содержит настройки фильтров содержимого для различных модулей и настроек фильтрации **WAF Dallas Lock**.
   - **UTM (Unified Threat Management).** Представляет собой межсетевой экран уровня логических границ сети и систему обнаружения вторжений уровня сети. Содержит настройки фильтров содержимого для различных модулей и настроек фильтрации **WAF Dallas Lock.**
   - **Настройки модуля ЕЦУ.** Обеспечивает взаимодействие между шлюзом безопасности **WAF Dallas Lock** и Единым центром управления Dallas Lock (ЕЦУ).
   - **Общие.** На данной странице администратор может задать основные параметры устройства, настройки учетных записей администратора и аудитора, логирование инцидентов безопасности и их передачу на удаленные серверы.
   - **Пользователи.** В **WAF Dallas Lock** реализован механизм управления доступом. **WAF Dallas Lock** может использоваться несколькими пользователями для выполнения разных функций. Также на странице отображен список заблокированных учетных записей пользователей, где разблокировка учетной записи пользователя осуществляется

автоматически по истечении указанного времени блокировки или после явной разблокировки администратором в разделе 5.5 Настройка пользователей.

- **Сервисы.** На странице реализована функциональная возможность включения почтовых уведомлений о событиях безопасности и настройка сторожевого таймера.
- **Управление сертификатами.** Представляет собой службу создания, обновления и замены цифровых сертификатов.
- **Аварийный режим.** На странице реализована функциональная возможность включения аварийного режима, проверки системы, установки порога превышения допустимого предела свободного дискового пространства, при превышении которого **WAF Dallas Lock** автоматически переходит в аварийный режим.
- **GEO IP фильтр.** Функциональная возможность настроить доступ к защищаемому ресурсу из определенных стран по геолокации на основе IP-адреса

4. **Сеть**
   - **Интерфейсы.** На данной странице представлены сетевые интерфейсы **WAF Dallas Lock** с указанием времени работы каждого из приведенных интерфейсов, его MAC-адреса, адреса IPv4 и IPv6 и полученные и переданные пакеты через этот интерфейс.
   - **DHCP и DNS.** Позволяют пользователю просмотреть активные аренды адресов по протоколу DHCP и DHCPv6, а также назначить постоянный или временный адрес определенному хосту. Пользователь может произвести дополнительные настройки служб DNS и DHCP.
   - **Имена хостов.** На данной странице пользователь может добавить имя и сетевой адрес хоста в зону DMZ.
   - **Статистические маршруты.** На данной странице пользователь может добавить статические маршруты по протоколам IPv4 и IPv6 для зарегистрированных в системе сетевых интерфейсов с указанием назначения маршрута (IP-адрес или сеть), маски подсети (если в предыдущей настройке была указана сеть), шлюза, метрики, максимального размера пакета и типа маршрута.
   - **Межсетевой экран.** На странице можно создать и настроить зоны в сети для контроля трафика. Страница содержит следующие вкладки:
     - *Основные* — отображает следующие настройки межсетевого экрана: входящий трафик, исходящий трафик, перенаправление.
     - *Перенаправление портов* — позволяет удаленным компьютерам из Интернета соединяться с компьютером или службой внутри частной локальной сети.
     - *Правила для трафика* — настройка правил для трафика, которые определяют политику прохождения пакетов между разными зонами.
     - *Правила аудита трафика* — настройка правил аудита трафика, которые определяют политику логирования проходящих пакетов между разными зонами.
     - *Списки доступа* — настройка списков доступа для блокировки сетей и хостов, являющихся источниками угроз для защищаемых ресурсов, а также для указания сетей и хостов, не подлежащих блокировке.
     - *Пользовательские правила* — настройка пользовательских правил, которые позволяют выполнять произвольные команды iptables, которые не охвачены рамками межсетевого экрана.
   - **Качество обслуживания (QoS).** На данной странице реализованы функциональные возможности по включению и отключению использования QoS, добавления сетевого интерфейса, на котором будет реализовываться качество обслуживания, а также добавления и удаления правил классификации QoS. Правила классификации могут быть настроены индивидуально для каждого интерфейса.
   - **Диагностика.** На данной странице расположена диагностика работы системы — возможность проверить целостность и качество соединения сети или выполнить трассировку маршрута и таким образом проверить доступность сервера, а также выполнить DNS-запрос.

5. **Перезагрузка.** При нажатии произойдет перезагрузка **WAF Dallas Lock**.

6. **Выйти.** Выйти из меню на страницу авторизации.

2 ПЕРВИЧНАЯ НАСТРОЙКА WAF DALLAS LOCK

2.1 Требование к техническому обеспечению

Изделие устанавливается на серверные платформы, работающие на базе процессорной архитектуры семейства x86_64, со следующими характеристиками:

- объем оперативной памяти должен составлять не менее 8 Гб, предпочтительно 16 Гб;
- количество ядер процессора должно быть не менее четырех с частотой 2 ГГц;
- объем памяти накопителя для хранения файлов регистрации журналов аудита должен быть не менее 32 Гб, предпочтительно 1Тб;
- количество сетевых карт должно быть не менее трех (LAN, WAN, DMZ);
- должно обеспечиваться наличие режима совместимости (MBR) в BIOS.

Установка **WAF Dallas Lock** возможна только на EFI BIOS.

2.2 Требование к сетевому соединению

Рекомендуемые требования к сетевому обеспечению:

- количество портов подключения RJ45 должно быть не менее двух со скоростью передачи данных не менее 1 Гб/с;
- количество портов подключения SFP+ должно быть не менее двух со скоростью передачи данных не менее 10 Гб/с.

2.3 Требование к программному обеспечению

Для корректной работы с графическим интерфейсом пользователя на рабочее место должен быть установлен один из следующих браузеров:

- Google Chrome 113 и выше;
- Mozilla Firefox 113 и выше;
- Microsoft Edge 104 и выше;
- Yandex 14 и выше.

2.4 Требование к среде виртуализации

WAF Dallas Lock может использоваться в виртуальной среде. Поддерживается установка **WAF Dallas Lock** из образа следующих виртуальных машин:

- VMware
- Hyper-V
- VirtualBox.

2.5 Процедура установки WAF Dallas Lock

В разделе описан алгоритм развертывания **WAF Dallas Lock** от момента установки и первого запуска, до внедрения в сеть и работы в штатном режиме с настройками по умолчанию.

Для установки **WAF Dallas Lock** необходимо:

- В загрузочном меню выбрать пункт **Install WAF Dallas Lock**, чтобы начать установку продукта (см. Рисунок 3);

Пункт **WAF Dallas Lock (Live CD)** *(*см. Рисунок 3), необходим исключительно для ознакомления с возможностями **WAF Dallas Lock**. Установка будет происходить в ОЗУ устройства.

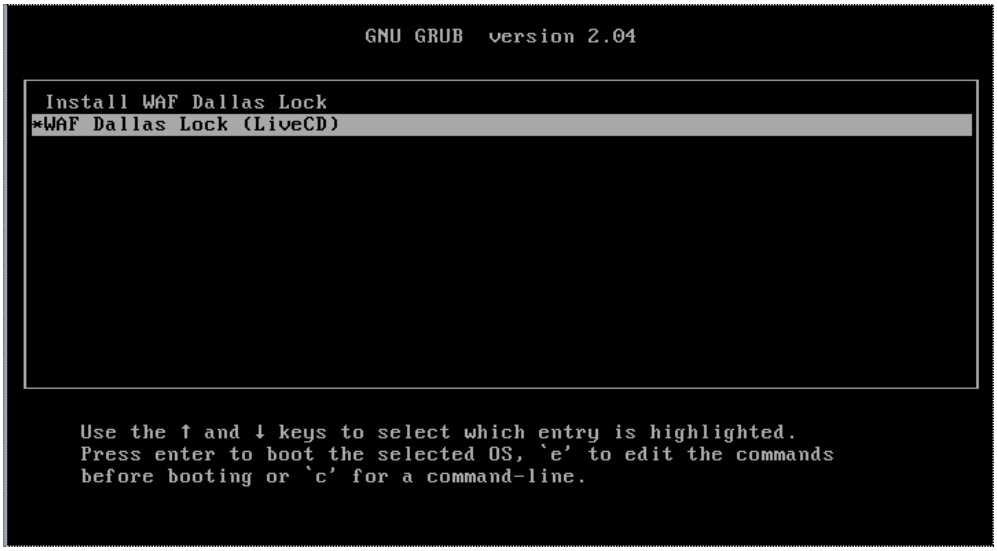


Рисунок 3. Загрузочное меню WAF Dallas Lock

- После загрузки с CD-ROM появится графическое консольное меню, где необходимо выбрать диск, на который будет осуществляться установка образа **WAF Dallas Lock** (см. Рисунок 4);
- Затем необходимо нажать кнопку **Установить** и в открывшемся окне подтвердить установку, нажав кнопку **Да**;

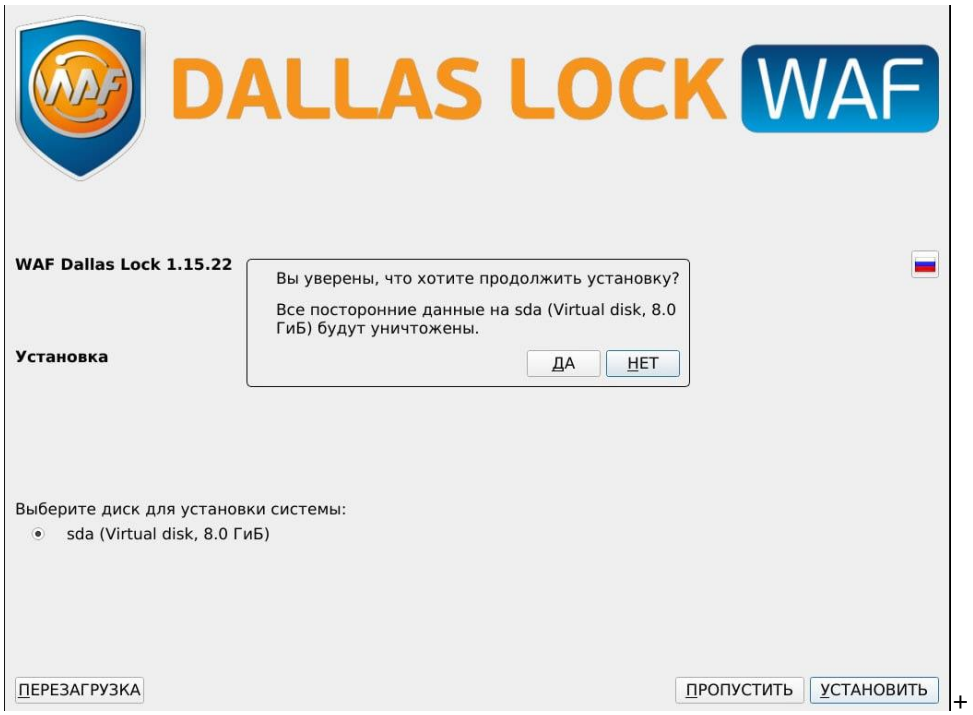


Рисунок 4. Выбор диска

Другие системы на выбранном диске будут удалены.

- После чего начнется процесс записи образа изделия на жесткий диск, необходимо дождаться завершения процесса установки;
- По окончании процесса установки необходимо перезагрузить ТС, нажав кнопку **ОК** в появившемся окне (см.
- Рисунок 5) и извлечь установочный носитель;

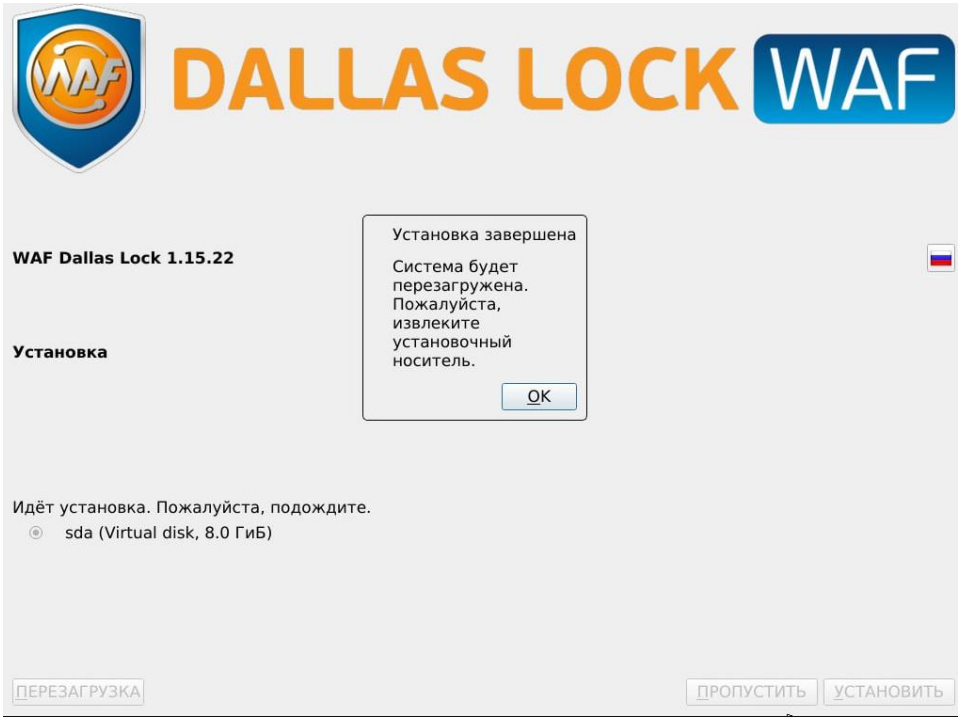


Рисунок 5. Перезагрузка

- Когда перезагрузка завершится, в загрузочном меню необходимо выбрать **WAF Dallas Lock** и на экране **Настройка** (см. Рисунок 6) ввести номер лицензии, код поддержки (см. в письме, отправленном на электронную почту) и сконфигурировать LAN-интерфейс сервера (предварительно рекомендуется настроить резервирование IP-адреса на DHCP-сервере);
- После ввода всех настроек необходимо нажать кнопку **Применить**, среда исполнения продолжит загрузку и по завершении процесса будет готова к последующим настройкам.

Рисунок 6. Меню первоначальной настройки WAF Dallas Lock

Номер лицензии с кодом технической поддержки, могут быть введены после установки и настройки **WAF Dallas Lock** в графической консоли администрирования, в меню **Настройки > Общие > Система > Лицензирование.**

- Если вы хотите сконфигурировать настройку сети вручную, например задать подсеть, шлюз и настроить сетевые интерфейсы необходимо нажать кнопку **Дополнительные настройки сети** (см. Рисунок 6);

  Маршрут до подсети управления. Задается статический маршрут из какой подсети или адреса пользователь будет иметь возможность подключения к веб-интерфейсу управления **WAF Dallas Lock**;

  Политики интерфейсов. Имя eth0 будет применятся для настройки данной сетевой карты. Где eth обозначает что используется Ethernet интерфейс, а 0 – номер устройства. Если у вас установлено несколько сетевых устройств, то соответственно им будут присвоены имена: eth0, eth1, eth2.

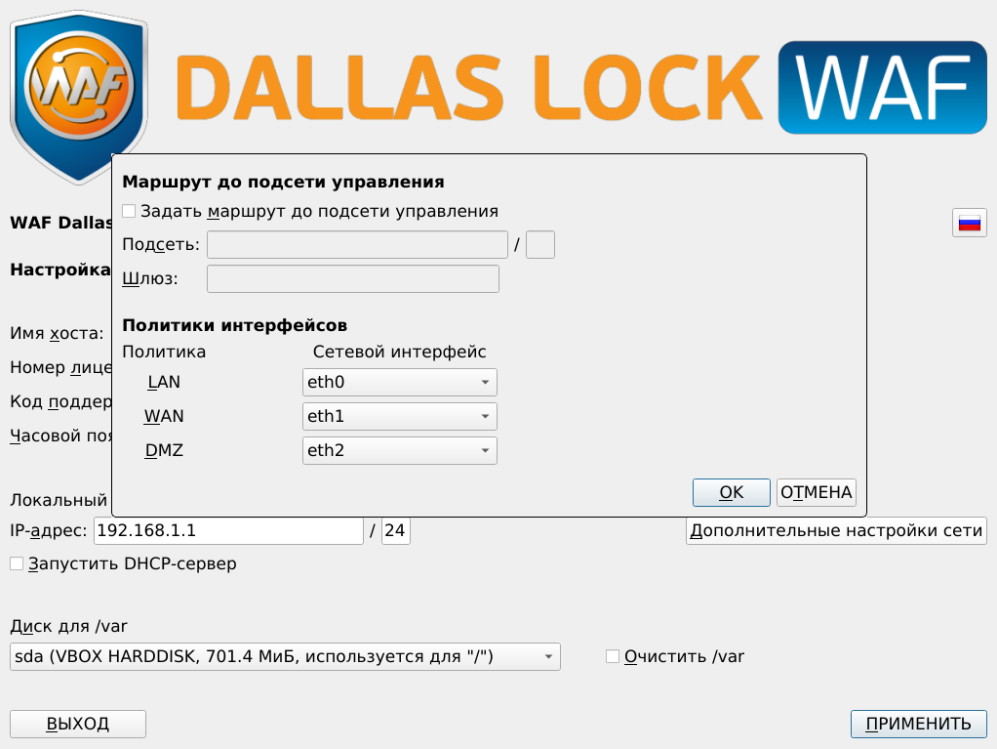


Рисунок 7. Дополнительные настройки сети

Доступ к средствам администрирования.

Чтобы приступить к конфигурации **WAF Dallas Lock** необходимо:

- подготовить компьютер для доступа к **WAF Dallas Lock** с зарезервированным IP-адресом и имеющий веб-браузер в составе установленного ПО;
- физически соединить LAN-порт программно-аппаратного комплекса с компьютером настройки;
- подключиться через браузер к веб-интерфейсу **WAF Dallas Lock** по защищенному HTTPS-соединению https://IP:7443, где IP — адрес узла с установленным **WAF Dallas Lock**. Далее отобразится форма аутентификации с полями *Имя пользователя*, *Пароль* и кнопками ***Войти*** и ***Сбросить***;
- на странице аутентификации ввести идентификатор (логин) пользователя с ролью *Администратор* в текстовое поле *Имя пользователя.* По умолчанию *root*. Поле *пароль* необходимо оставить пустым. Нажать кнопку **Войти**. (см. Рисунок 8);

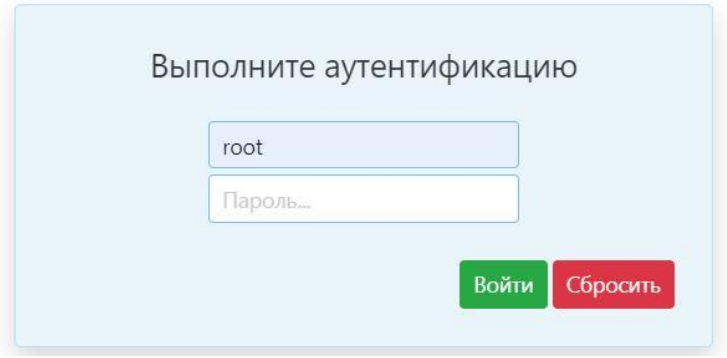


Рисунок 8. Аутентификация пользователя

- для создания или генерации пароля суперпользователя (администратора) **WAF Dallas Lock** будет автоматически перенаправлено на страницу настройки интерфейса управления (см. Рисунок 9).

Если не будет задан пароль суперпользователя (администратора), переход на другие страницы статистики и настройки **WAF Dallas Lock** будет невозможен.

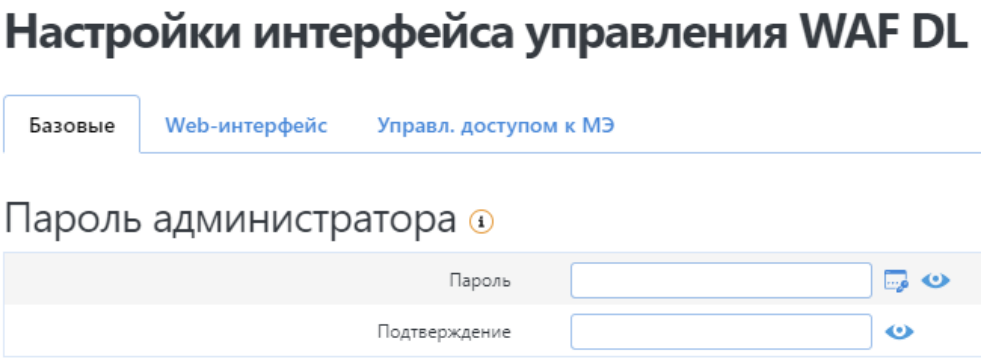


Рисунок 9. Создание пароля администратора

Пароль не может быть короче 8 символов, должен соответствовать требованиям безопасности и содержать:

- символы нижнего регистра;
- символы верхнего регистра;
- минимум одна цифра;
- специальный символ.

2.6 Лицензирование продукта

Для защиты от нелегального использования продукта необходимо ввести номер лицензии, указанный на коробке компакт-диска с дистрибутивом **WAF Dallas Lock**, и код технической поддержки, который указан в письме, отправленном на электронную почту.

Действующий код технической поддержки является условием предоставления помощи в установке и настройке **WAF Dallas Lock** специалистами компании-разработчика, а также условием доступа к сертифицированным обновлениям.

2.7 Добавление защищаемого ресурса

Для того, чтобы добавить защищаемый ресурс, необходимо в пункте основного меню выбрать **Настройки**, перейти на вкладку **WAF** и выбрать в меню третьего уровня *Инспекция WAF* (см. Рисунок 10).

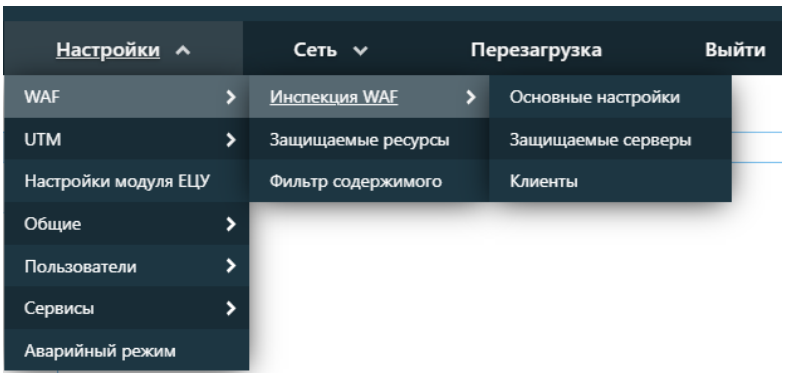


Рисунок 10. Инспекция WAF

Далее на странице *Инспекция WAF* перейти на вкладку *Защищаемые серверы*. Нажать на кнопку **Добавить**. В поле *IP-Адреса* добавить веб-узел защищаемого объекта и в поле *Описание* задать имя веб-узла. Нажать на кнопку **Применить** (см. Рисунок 11). Подробное описание функциональных возможностей настроек на вкладке *Защищаемые серверы* в разделе 5.1.1 Инспекция WAF.

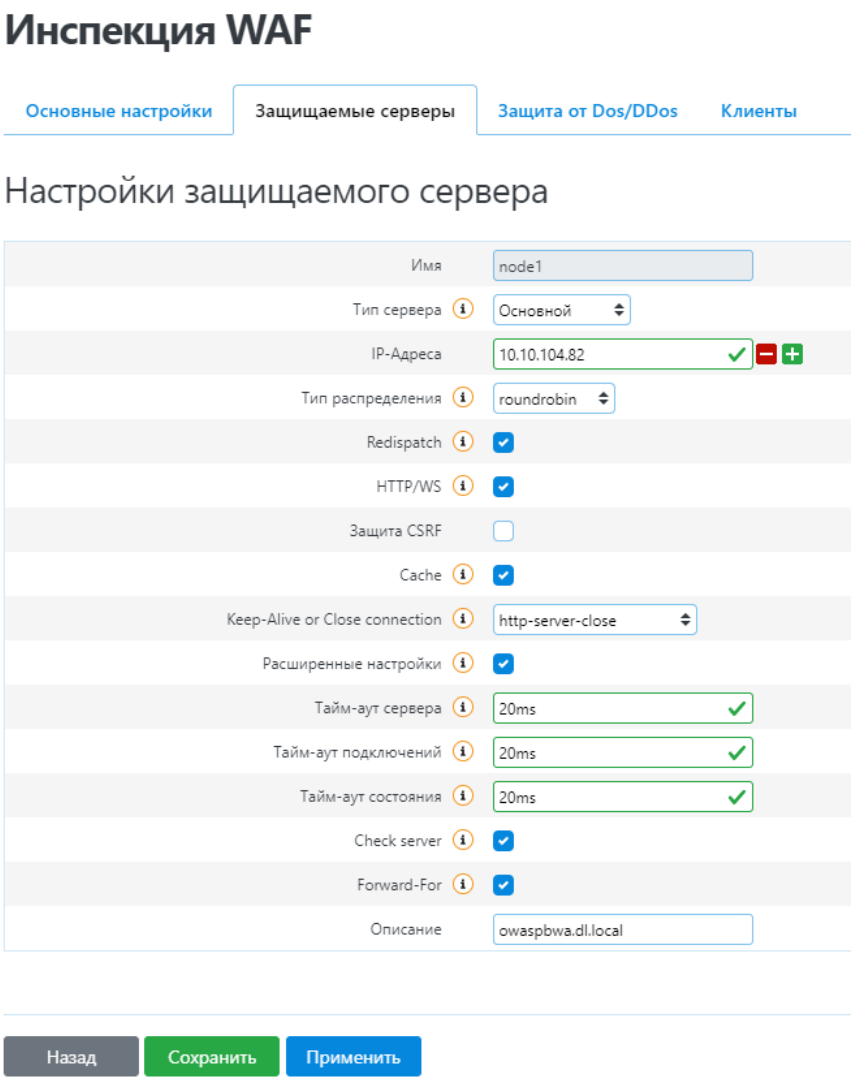


Рисунок 11. Добавление защищаемого объекта

После сохранения защищаемый объект автоматически добавляется в список на вкладке *Защищаемые серверы* (см. Рисунок 12).

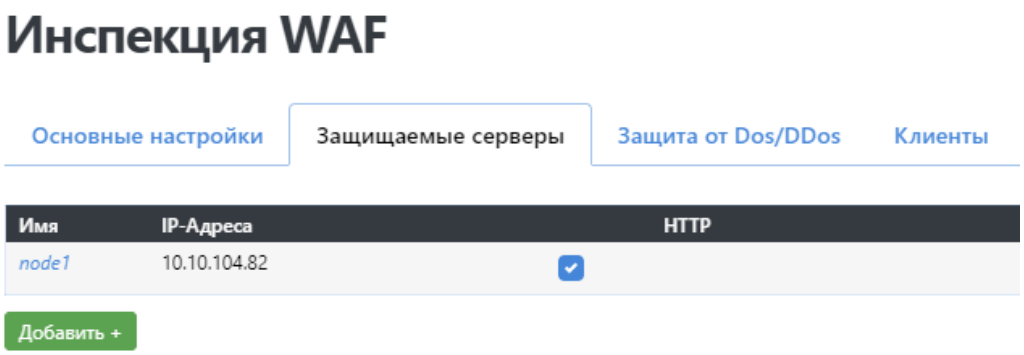


Рисунок 12. Список защищаемых объектов

После того как добавили защищаемый ресурс, нужно перейти в **Настройки > WAF > Защищаемые ресурсы** и добавить корневой сертификат Удостоверяющего центра (см. Рисунок 13). Более подробное описание настройки смотреть в разделе 5.1.1 Инспекция WAF.

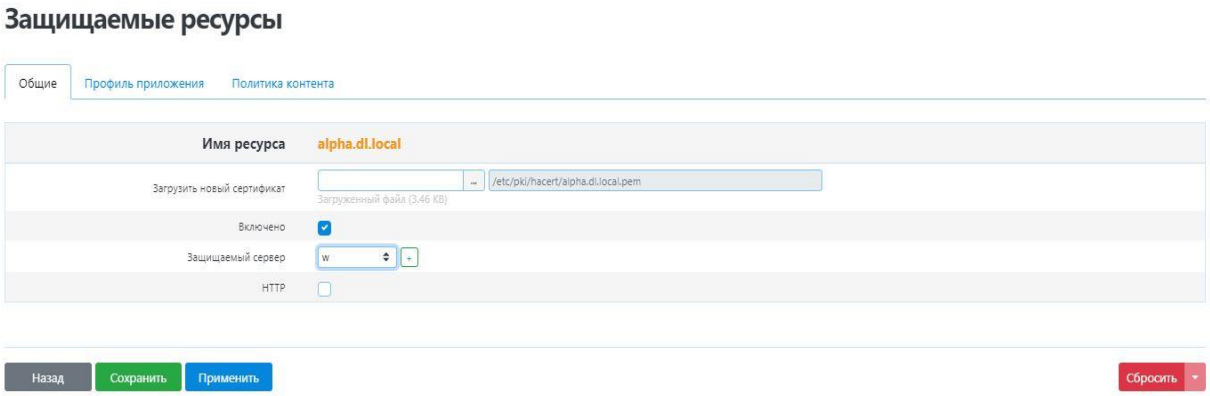


Рисунок 13. Добавление сертификата

Далее переходим на вкладку *Профиль приложения*, чтобы задать механизмы защиты, которые нас интересуют.

Внедрение веб-сервера в DMZ

Внедрение веб-серверов в DMZ сводится к обеспечению физической и логической IP-связности с **WAF Dallas Lock**, а также настройке поддержки работы протоколов HTTP и HTTPS, и проверяется успешным отображением веб-страницы сервера из DMZ при обращении к **WAF Dallas Lock** со стороны WAN-зоны. При необходимости проверяется связность с LAN-зоной отображением веб-страниц на хостах LAN-зоны, отсутствием возможности со стороны веб-сервера инициировать соединения с LAN-хостами и отобразить веб-интерфейс настройки **WAF Dallas Lock**.

Для добавления веб-сервера в DMZ следует выполнить следующие шаги:

- подготовить веб-сервер и его SSL-сертификаты в формате PEM;
- физически соединить кабелем **WAF Dallas Lock** и подключаемый веб-сервер;
- обеспечить IP-связность заданием на сервере IP-адреса из сети 172.16.16.0/24 и маршрута по умолчанию 172.16.16.1;
- на странице **Сеть** — **Интерфейсы** убедиться в отображении веб-сервера среди клиентов в DMZ;
- загрузить в **WAF Dallas Lock** сертификаты веб-сервера;
- указать номер порта на WAN-интерфейсе для приема HTTPS-соединений к веб-серверу;
- указать IP-адрес, порт и имя хоста веб-сервера для обеспечения ретрансляции соединений, принимаемых на WAN-интерфейс;
- проверить отображение веб-страницы, передаваемой веб-сервером обращением со стороны WAN-зоны **WAF Dallas Lock** в соответствии с указанными настройками трансляции адресов;
- проверить установление веб-сервером защищенного (HTTPS) соединения с **WAF Dallas Lock** при обработке запросов средствами веб-сервера.

При необходимости проверить:

- отсутствие отображения веб-страницы **WAF Dallas Lock** со стороны WAN-зоны при физически отключенном веб-сервере;
- отсутствие отображения веб-интерфейса **WAF Dallas Lock** при запросе со стороны веб-сервера;
- отображение веб-страницы, передаваемой веб-сервером, обращением со стороны хоста из LAN-зоны по IP-адресу веб-сервера в DMZ.

3 ИНФОРМАЦИОННАЯ ПАНЕЛЬ

Блок основной информации по атакам содержит: пять виджетов с кольцевыми диаграммами, один виджет с информацией об аппаратном обеспечении системы, четыре — с графиками и один — со списком инцидентов.

3.1 Виджет «Атакуемые ресурсы»

Виджет с кольцевой диаграммой, на котором отображены наиболее атакуемые ресурсы из списка защищаемых (см. Рисунок 14).

При нажатии на какой-либо ресурс, он отображается на виджете **Атаки, зафиксированные на ресурсы**. На виджете **Атакуемые ресурсы** может отображаться не более 10 записей.

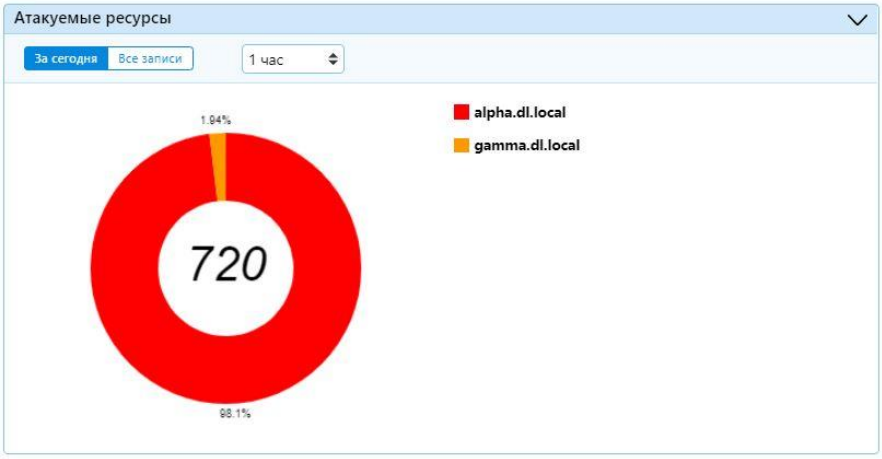


Рисунок 14. Виджет «Атакуемые ресурсы»

3.2 Виджет «Аппаратное обеспечение»

Виджет **Аппаратное обеспечение** (см. Рисунок 15) содержит данные в реальном времени о нагрузке на CPU, свободном объеме оперативной памяти и месте на устройстве для постоянного хранения информации, а также среднюю загрузку системы.

Рисунок 15. Виджет «Аппаратное обеспечение»

Методом отображения уровня загрузки аппаратного обеспечения служит динамически изменяемый индикатор выполнения с цифровым и/или процентным обозначением по середине. Для процессора это процентное обозначение. Для ОЗУ указывается значение «занятая память/ всего памяти (занято памяти в процентах)» в гигабайтах. Для места на диске указывается значение «занято место на диске / всего места на диске (занято места в процентах)» в гигабайтах. Для упрощения отображения процентные соотношения приведены в целых числах, объем диска

представлен в виде десятичной дроби.

3.3 Виджет «Все зафиксированные атаки»

Виджет с кольцевой диаграммой (см. Рисунок 16), на котором отображены девять наиболее массовых (по количеству) атак, обнаруженных межсетевым экраном типа Г (WAF), на все защищаемые ресурсы.

На виджете реализована функциональная возможность выборки по диапазону дат, а также выборка за сегодняшнюю дату или отображение зафиксированных атак за все время. При применении какой-либо выборки на данном виджете. Ее результаты автоматически применяется на виджетах **Источники атак** и **Атакуемые ресурсы**.

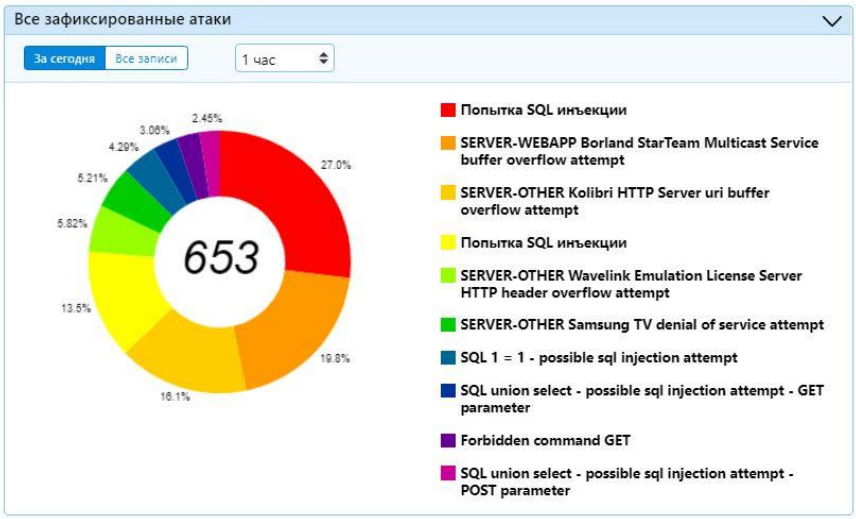


Рисунок 16. Виджет «Все зафиксированные атаки»

3.4 Виджет «Источники атак»

Виджет с кольцевой диаграммой, на котором отображены источники всех зафиксированных атак (см. Рисунок 17).

На данном виджете представлены сетевые адреса источников, с которых зафиксировано максимальное количество атак. Содержимое данной диаграммы не всегда может соответствовать содержимому диаграммы виджета **Все зафиксированные атаки**, так как с различных адресов (источников атак) зафиксирован один вид атаки. Аналогично диаграмме атак, диаграмма источников подписана количеством атак (и/или процентным соотношением) с данного источника (IP-адреса). Цвет сектора диаграммы соответствует цвету источника атак в легенде.

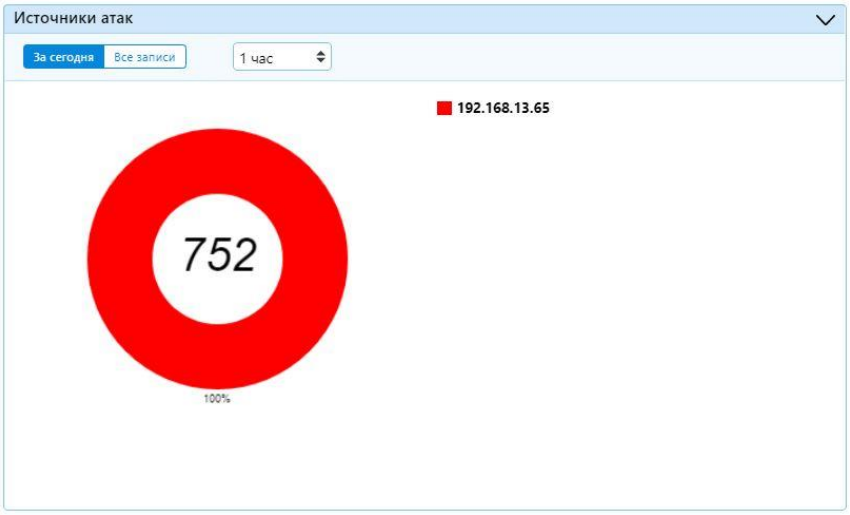


Рисунок 17. Виджет «Источники атак»

3.5 Виджет «Атаки, зафиксированные на ресурсы»

Виджет содержит кольцевую диаграмму с источниками, по которым выводятся атаки, либо указываются вручную при помощи кнопки **Изменить ресурсы**. При нажатии кнопки **Изменить ресурсы**, пользователю выводится текстовое поле, в которое он может вписать наименование защищаемого ресурса и подтвердить ввод кнопкой **Сохранить** (см. Рисунок 18).

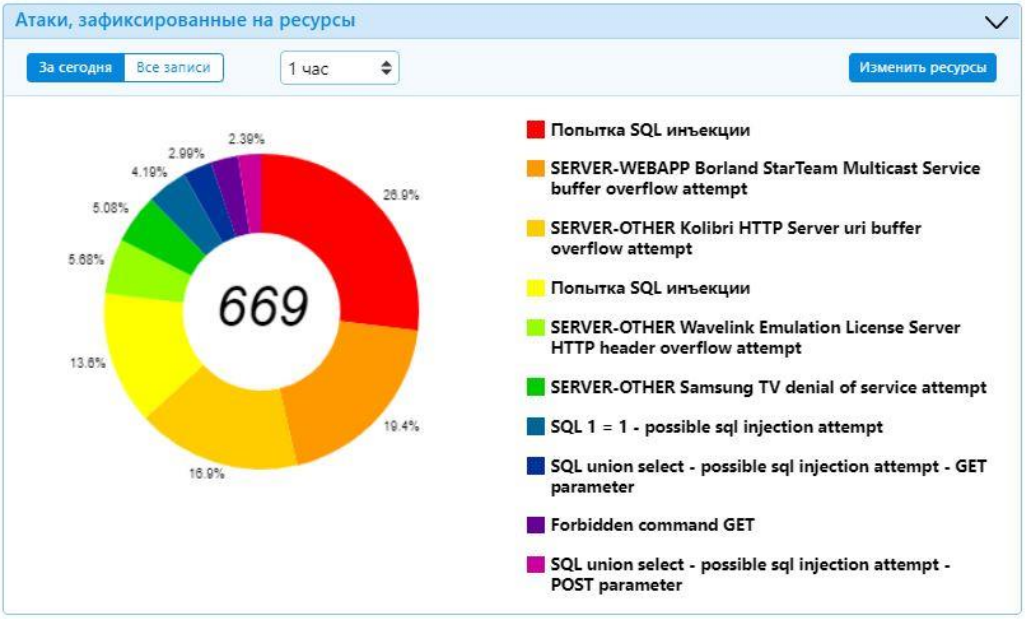


Рисунок 18. Виджет «Атаки, зафиксированные на ресурсы»

3.6 Виджет «Источники атак, зафиксированные на ресурсы»

Виджет содержит кольцевую диаграмму с источниками, с которых были зафиксированы атаки на наблюдаемые ресурсы (ресурсы, которые были добавлены в виджет **Атаки, зафиксированные на ресурсы**) (см. Рисунок 19).

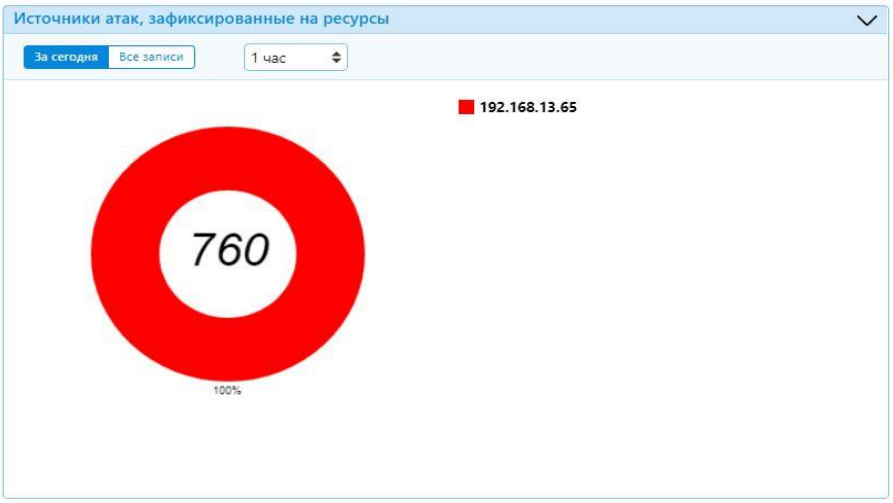


Рисунок 19. Виджет «Источники атак, зафиксированные на ресурсы»

3.7 Виджет «Уровни тревоги атак»

В данном виджете, на основании анализа зафиксированных атак, проводимого в режиме реального времени при получении новых данных, отображенных на кольцевой диаграмме атак, строятся графики уровней тревоги зафиксированных атак за выбранный период.

Вертикальная ось обозначает количество зафиксированных атак, где максимальное число на оси

равно максимальному количеству атак, отображаемых за период. Горизонтальная ось — ось времени, сегментированная на части, в зависимости от выбранного периода времени, цена деления которой зависит от результата выборки на виджете **Все зафиксированные атаки.**

*будет кратна четырем. Например, если выбран период в 13 дней, то цена деления равна 4-м дням (16/4), а график строится на выбранный период. При этом цена деления вычисляется исходя из увеличения выбранного числа неделимого на 4 без остатка до числа, делимого на 4 без остатка, делением этого числа на 4 (см. Рисунок 20).

Уровни подразделяются на высокий, средний и низкий. График каждого уровня опасности имеет свой цветовой окрас: красный, синий и зеленый соответственно.

Если атаки (атака) относятся к одному уровню, на графике отображается только один график из трех возможных. Аналогично при наличии атак, относящихся только ко двум уровням тревоги. При отсутствии выбранных типов атак или выбранных, но не зафиксированных типах атак, график остается пустым.

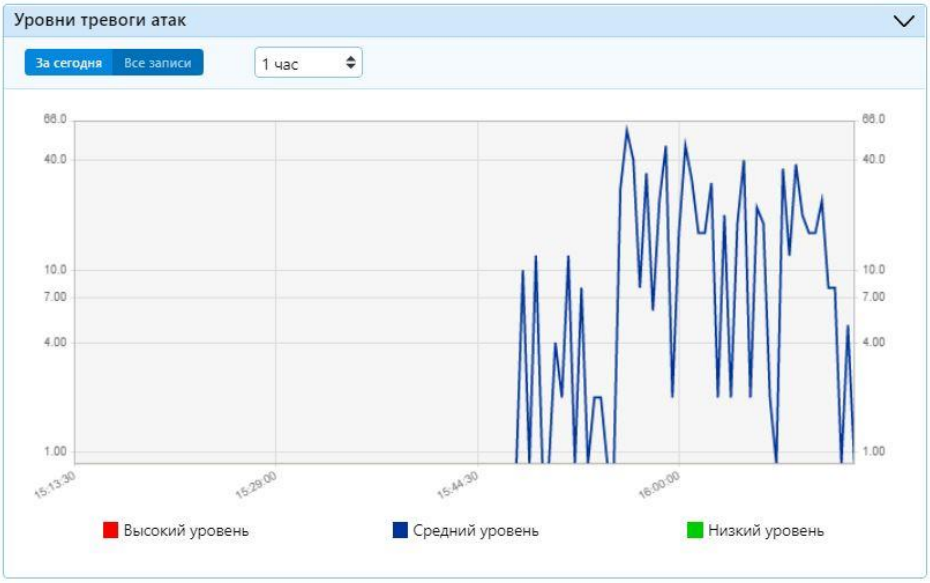


Рисунок 20. Виджет «Уровни тревоги атак»

3.8 Виджет «Уровни тревоги атак, зафиксированные на ресурсы»

Ресурсы, по которым выводятся атаки, либо указываются вручную при помощи кнопки **Добавить ресурс**, либо кликом левой кнопкой мыши по имени ресурса на виджете **Атакуемые ресурсы**. При нажатии кнопки **Добавить ресурс**, пользователю выводится текстовое поле, в которое он может вписать наименование защищаемого ресурса и подтвердить ввод кнопкой **Ок** или отменить ввод ресурса кнопкой **Отмена**. При вводе имени ресурса (включая указание «http://», «https://», «www» или без их указания), пользователю выводится список всех известных защищаемых ресурсов, соответствующих маске введенных данных. При выборе имени защищаемого ресурса из выводимого списка все символы «обрезаются» до имени домена. Если совпадений нет — пользователю будет выведено сообщение *Не найдено.*

Удаление ресурса из списка наблюдаемых происходит путем раскрытия выпадающего меню с именами защищаемых ресурсов на данном виджете и нажатием символа с крестиком напротив его имени (при этом кольцевая диаграмма будет перестроена).

Данный виджет содержит не более десяти защищаемых ресурсов. Удаление ресурса из списка производится путем выбора его из выпадающего списка и нажатием на кнопку с крестиком напротив его наименования. Если никаких ресурсов не указано, то выводится пустая кольцевая диаграмма, а в легенде выводится надпись *Добавьте защищаемый ресурс.*

При добавлении ресурса с виджета **Атакуемые ресурсы**, пользователю выводится сообщение с подтверждением или отменой действия. В случае переполнения списка ресурсов, после подтверждения действия добавления ресурса, пользователю выводится список ресурсов, уже содержащихся на виджете **Атаки, зафиксированные на ресурсы** для редактирования, в котором пользователь может удалить один или несколько ресурсов.

Для каждого добавленного защищаемого ресурса на круговой диаграмме отображена проводимая

на него атака. На один ресурс может быть зафиксировано несколько различных атак и все они отображены в процентном соотношении на кольцевой диаграмме. При добавлении ресурса, на который зафиксированы атаки отличные от атак на ресурс, добавленный ранее, на кольцевой диаграмме отражается долевое соотношение всех атак на указанные ресурсы (см. Рисунок 21).

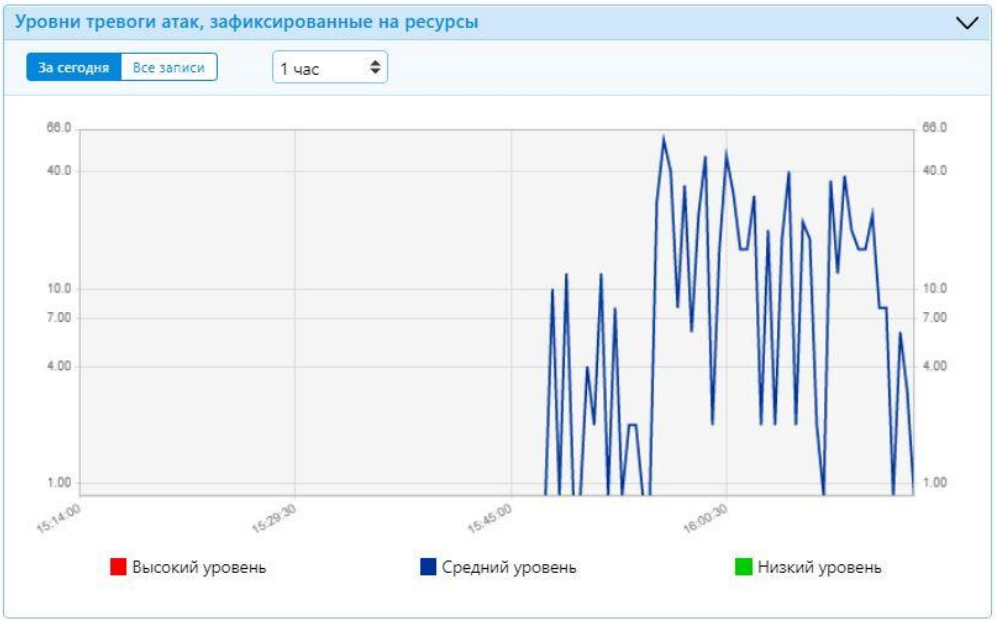


Рисунок 21. Виджет «Уровни тревог атак, зафиксированные на ресурсы»

3.9 Блок «Список инцидентов»

Блок **Список инцидентов** (см. Рисунок 22) должен содержать в себе зафиксированные данные по инцидентам безопасности, относящимся только к событиям МЭ типа Г, а также инструментарий для поиска и сортировки этих данных.

Блок **Список инцидентов** содержит следующие элементы управления:

- *Уровень атак* (все, высокий, средний, низкий) — при выборе какого-либо значения, список содержит либо все данные по атакам, либо сортирует их по уровню — высокий, средний, низкий. По умолчанию установлено значение *Все*.
- *Диапазон дат* — список инцидентов содержит данные за выбранный период, при выборе пункта *Вчера***,** отобразятся все инциденты за вчерашний день, при выборе пункта *Сегодня* — за сегодняшний. По умолчанию в списке отображаются все зафиксированные инциденты (пункт *Все записи*).
- *Показать* — данный параметр регулирует количество записей, отображаемых в блоке в один момент времени. Может принимать значение 10, 25, 50, 100 записей. Минимальное количество записей, отображаемых в блоке — 10. При увеличении количества записей блок не увеличивается, для пролистывания записей применяется полоса прокрутки.
- *Скачать* — при нажатии пользователь получает возможность загрузить на локальный носитель результат выборки данных из списка инцидентов или весь список целиком в текстовом формате.
- *Сбросить* — при нажатии происходит сброс всех фильтров на значения по умолчанию.
- *Поиск* — данная строка используется для поиска текстовых данных в списке инцидентов безопасности, к которому применены параметры сортировки.
- *Количество страниц* (страничная очередь) < 1 | 2 | 3 … 15 > — данный параметр отображения позволяет пользователю производить навигацию между страницами, содержащими инциденты безопасности. Количество страниц зависит от количества инцидентов безопасности всего и количества инцидентов безопасности, отображаемых в данный момент, определенного параметром *Показать.*

Отображаемая таблица с данными содержит следующие поля:

- ID — уникальный идентификатор записи инцидента.

- Время — дата и время в формате ДД.ММ.ГГГГ ЧЧ:ММ:СС каждого зафиксированного инцидента.
- Событие — описание события инцидента.
- Информация — дополнительная информация о зафиксированном инциденте, заполняется в случае необходимости.

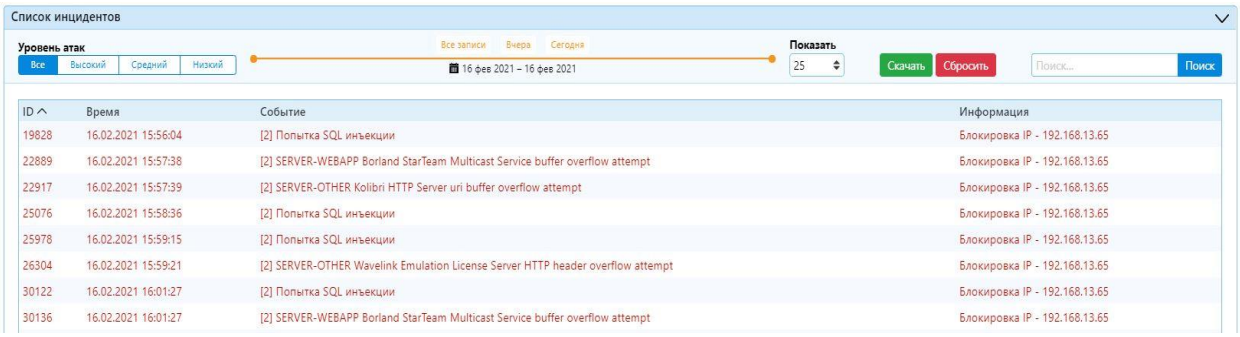


Рисунок 22. Блок «Список инцидентов»

3.10 Виджет «Трафик в реальном времени»

Виджет **Трафик в реальном времени** представлен в виде графика входящего и исходящего трафика по интерфейсам (см. Рисунок 23).

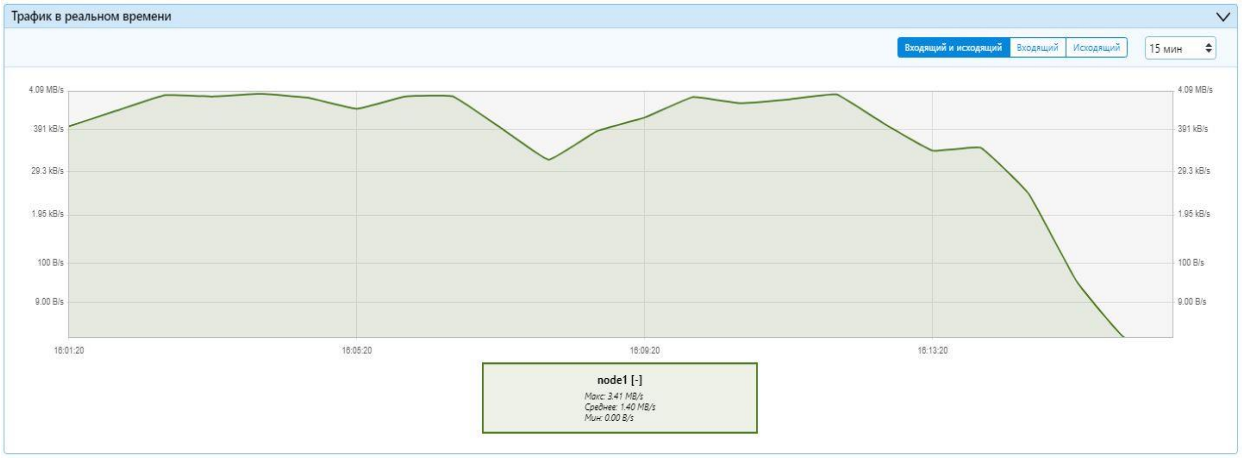


Рисунок 23. Виджет «Трафик в реальном времени»

Источником данных для графика являются или ресурсы, выбранные на виджете **Атаки, зафиксированные на ресурсы**, или перечень из наиболее загруженных ресурсов. Если выбран источник данных **Атаки, зафиксированные на ресурсы**, то под каждым наименованием ресурса размещены минимальные, средние и максимальные значения данных, отображаемых на графике.

На графике **Трафик в реальном времени** представлена легенда, на которой указаны входящие и исходящие объемы фиксируемого трафика, а также их средние и пиковые показатели.

3.11 Виджет «Запросы в реальном времени»

На графике **Запросы в реальном времени** (см. Рисунок 24) по горизонтали представлена сетка интервала, по которому отображается график, а также элемент управления, с помощью которого уполномоченный пользователь может изменять сам интервал. Интервал может быть задан следующими показателями — 3 минуты, 15 минут, 30 минут, 1 час, 3 часа, 6 часов, 12 часов, 24 часа. Так же на виджете представлена легенда, на которой указано количество подключений TCP. А также средние и пиковые значения для каждого типа подключений.

Источником данных для графика являются или ресурсы, выбранные на виджете **Атаки, зафиксированные на ресурсы**, или перечень из наиболее загруженных ресурсов.

Рисунок 24. Запросы в реальном времени

4 ЖУРНАЛЫ И СТАТИСТИКА

Ведение журналов информационной безопасности в **WAF Dallas Lock** позволяет обеспечивать необходимый уровень защиты, предоставляя и накапливая в хронологическом порядке важную информацию о состоянии системы защиты, событиях работы пользователей, событиях изменения политик безопасности и настроек прав доступа. Архивы таких журналов предоставляют необходимую базу для расследования инцидентов нарушения информационной безопасности.

Для отображения событий безопасности также применяют графические оповещения, оповещения по электронной почте, системы оперативного мониторинга. В данном разделе рассмотрены состав, доступ и настройка журналов и статистики, а также состав и назначение полей этих журналов.

4.1 Журналы аудита

Меню **Журналы и статистика** графического интерфейса **WAF Dallas Lock** содержит пункт **Журналы аудита** (см. Рисунок 25), нажав на который пользователь переходит на страницу со следующими журналами:

- Журнал *Инциденты* — содержит данные по инцидентам безопасности, зафиксированным **WAF Dallas Lock**.
- Журнал *WAF* — содержит события, основанные на сигнатурном анализе правил для межсетевого экрана уровня приложений.
- Журнал *СОВ* — содержит события, связанные с подозрительной (опасной) активностью сетевых приложений (в том числе веб-ресурсов) и пользователей, основываясь на сигнатурном и эвристическом методах анализа данных, проходящих через **WAF Dallas Lock.**
- Журнал *МЭ* — содержит события, основанные на сигнатурном анализе правил для межсетевого экрана уровня границы сети.
- Журнал *Сетевые пакеты* — содержит события, связанные с передачей пакетов данных по всем протоколам.
- Журнал *Политики* — содержит данные о модификации политик безопасности **WAF Dallas Lock**, в том числе отклоненные данные (значения данных, которые не подходят по формату поля, являются не безопасными и т.п.) и данные о создании, модификации и удалении учетных записей пользователей **WAF Dallas Lock**.
- Журнал *Авторизация* — содержит информацию о попытках (удачных и неудачных) входа пользователей в графический интерфейс и консоль **WAF Dallas Lock**.
- Журнал *Системный* — содержит события системы **WAF Dallas Lock**, в том числе системные сообщения, сообщения процессов и сообщения планировщика заданий.
- Журнал *Прокси* — отображает данные как по HTTP-запросам к веб-серверу, так и по ответам, полученным от веб-сервера.

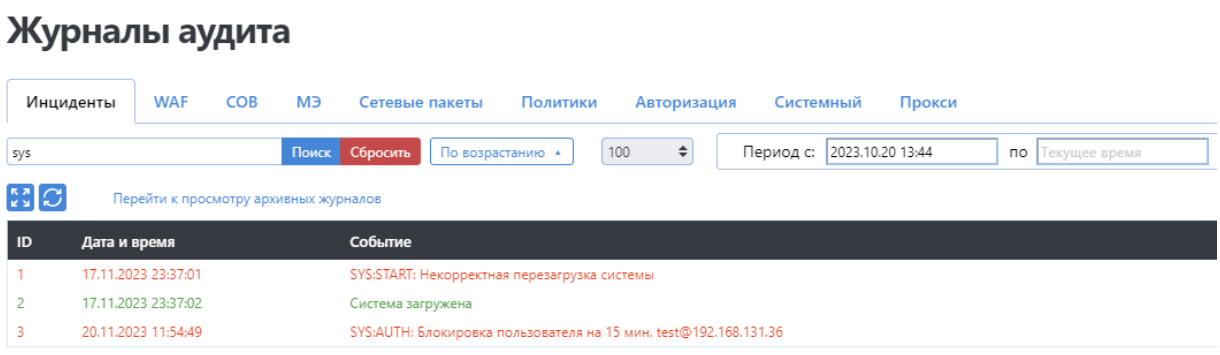


Рисунок 25. Журналы аудита

4.1.1 Доступ к журналам аудита

Доступ к журналам аудита предоставляется только уполномоченным пользователям (определенным учетным записям) в строгом соответствии с назначенными правами доступа. Проверка прав доступа учетной записи пользователя производится при входе пользователя в веб-

интерфейс. Настройка прав доступа осуществляется администратором системы на странице конфигурации пользователей.

Учитывая, что МЭ, WAF и СОВ являются отдельно лицензируемыми модулями, пользователям отображаются только те журналы аудита, модули которых были лицензированы.

Доступ или отказ в доступе к журналам аудита, все модификации настроек журналов аудита пользователями, а также сбои хранения журналов (в части фиксации сообщения *Журнал заканчивается* при 80% занятого дискового пространства, сообщения *Журнал закончился* при 90% занятого дискового пространства) и предпринимаемые действия при сбоях хранения журналов фиксируются в журнале *Управление политиками*.

Сбой журналирования системы заносится в *Аварийный журнал*.

4.1.2 Содержание журналов аудита

Каждый журнал аудита содержит набор полей, в которые вносятся данные, относимые к тому или иному событию. Состав полей журналов, представлен в таблице 1.

Таблица 1. Список полей журналов аудита

Наименование журнала	Список полей
Инциденты	ID — уникальный номер записи журнала (идентификатор события) Дата и время Событие Информация Результат[1]
WAF	ID — уникальный номер записи журнала (идентификатор события) Дата и время Событие Источник Направление Протокол Сигнатура Результат Информация
СОВ	ID — уникальный номер записи журнала (идентификатор события) Дата и время Событие Источник Направление Протокол Сигнатура Результат Информация
МЭ	ID — уникальный номер записи журнала (идентификатор события) Дата и время Событие Источник

[1] Поле *Результат* журнала *Инциденты* всегда будет содержать значение *Ок*, в связи с тем, что не идентифицированный инцидент отражен быть не может.

	Направление Протокол Сигнатура Результат Информация
Сетевые пакеты	ID — уникальный номер записи журнала (идентификатор события) Дата и время Источник Направление Протокол Результат Информация
Политики	ID — уникальный номер записи журнала (идентификатор события) Дата и время Пользователь Информация Результат
Авторизация	ID — уникальный номер записи журнала (идентификатор события) Дата и время Пользователь Информация Результат
Системный	ID — уникальный номер записи журнала (идентификатор события) Дата и время Событие Объект Информация Результат
Прокси	ID — уникальный номер записи журнала (идентификатор события) Дата и время Событие Объект Информация Результат

4.1.3 События журналов аудита

При наступлении какого-либо события, **WAF Dallas Lock** формирует запись в журнал аудита, относящуюся к тому или иному событию. Общее описание журналируемых событий, при наступлении которых формируется запись в соответствующий журнал, представлено в таблице 2.

Таблица 2. Список журналируемых событий

Наименование журнала	Список полей
Инциденты	Зафиксированные инциденты безопасности Запись реакции на группу событий эвристики СОВ
WAF	Срабатывания правил WAF (например, правила, защищающие от угроз OWASP10)

СОВ	Срабатывание правил эвристического анализа СОВ Срабатывание сигнатур СОВ
МЭ	Срабатывание сигнатур МЭ
Сетевые пакеты	Фиксация сетевых пакетов
Политики	События модификации политик Создание, модификация, удаление пользователей Изменение пароля пользователя Блокировка учетной записи пользователя Разблокировка учетной записи пользователя Получение пользователем доступа к журналам Отказ в доступе к журналу аудита Модификация настроек журналирования
Авторизация	Вход/выход учетной записи пользователя
Системный	События системного журнала SysLog События планировщика событий (cron) События по запуску/остановке процессов в автоматическом режиме События старт/остановка/сбой работы/возврат или не возможность возврата к безопасному состоянию (если аудит возможен) системы Факт выгрузки журналов через интерфейс Иные системные сообщения
Прокси	События по HTTP-запросам к защищаемым ресурсам

4.1.4 Сортировка записей аудита

В каждом из вышеописанных журналов аудита реализована возможность фильтрации и сортировки записей аудита:

- Поле поиска (Фильтр…) позволяет сделать выборку по записям аудита. Для выведенных строк фильтрация осуществляется «на лету». Чтобы поиск был осуществлен по всему журналу, и отобразились все строки, содержащие текст запроса — необходимо нажать кнопку **Поиск** (см. Рисунок 26).
- Сортировка записей аудита по убыванию и по возрастанию. При нажатии на кнопку сортировки **По убыванию** происходит фильтрация журнала по убыванию, основанная на дате и времени события, при этом наименование кнопки изменяется на **По возрастанию**, нажатие на которую приводит к сортировке журнала по возрастанию (см. Рисунок 26).

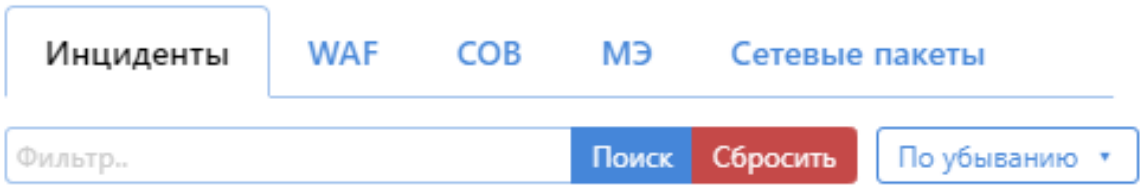


Рисунок 26. Поиск и сортировка событий.

Журналы аудита отображаются в виде таблицы. Во всех журналах предусмотрена возможность выбора количества отображаемых событий на странице: от 25 до 500. Кроме того, в каждом из журналов (за исключением журнала *Прокси*) реализована возможность выбора отображаемого периода (см. Рисунок 27).

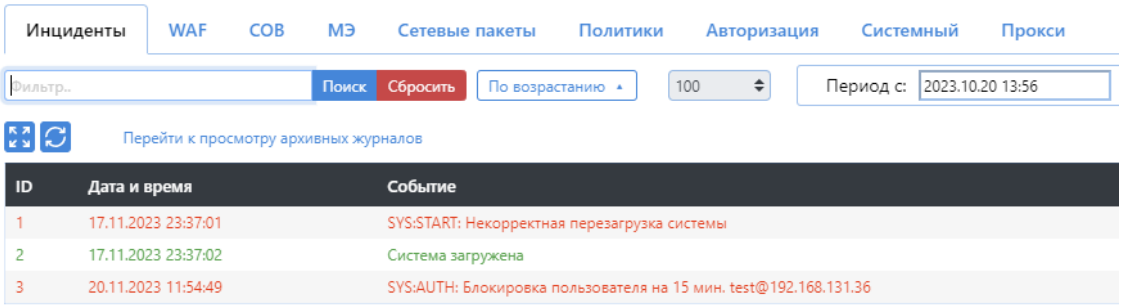


Рисунок 27. Количество отображаемых событий и выбор периода

При отсутствии совпадения данных в журнале с данными из поискового запроса, пользователю выводится пустой журнал. Возвращение к первоначальному представлению журнала в пользовательском интерфейсе происходит путем нажатия на кнопку **Сбросить**.

Во всех журналах (за исключением журнала *Прокси*) доступна фильтрация и отображение событий по их результату: Ок (успешно), предупреждение, ошибка (см. Рисунок 28).

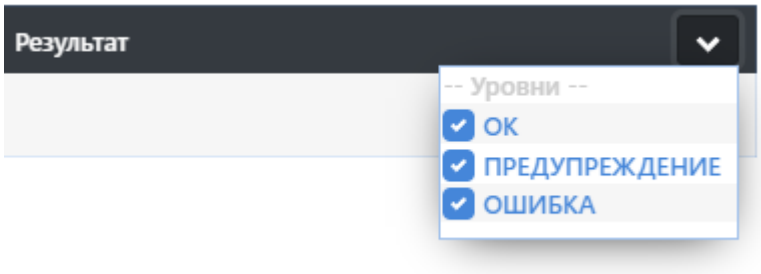


Рисунок 28. Фильтрация и отображение событий

В журнале *Прокси* по умолчанию отображаются все события. Чтобы в списке отобразились только запросы с ошибками и предупреждениями, необходимо включить переключатель в режим *Только ошибки* (см. Рисунок 29).

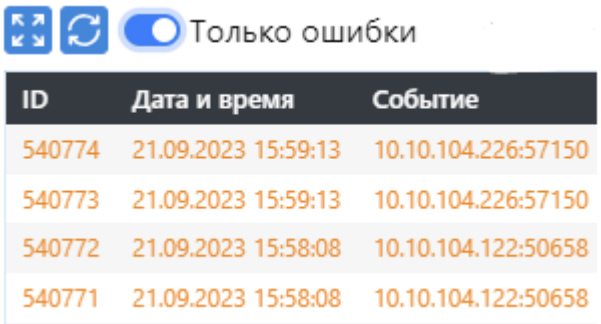


Рисунок 29. Отображение списка ошибок и предупреждений

Кнопка **Сохранить** производит выгрузку активного журнала с учетом поискового запроса из строки *Фильтр* и с сохранением порядка сортировки.

4.1.5 Выгрузка журналов аудита

При выборе какого-либо журнала, осуществляется выгрузка записей журнала, путем нажатия на соответствующую кнопку **Выгрузить активный журнал**. Факт выгрузки активного журнала фиксируется в *системном* журнале.

Выгрузка журнала осуществляется в текстовом формате и предложена пользователю для скачивания через веб-браузер.

4.3 Журнал ядра

Страница (см. Рисунок 30) содержит выборку данных из журнала ядра системы. Журнал представлен в текстовом виде, имеет функциональные возможности поиска, сортировки по убыванию и возрастанию, и сброс фильтров. Сохранение журнала доступно путем копирования текста в буфер обмена.

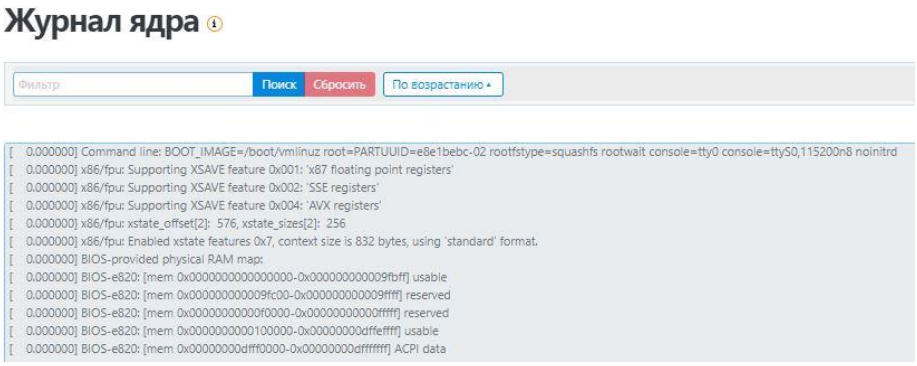


Рисунок 30. Журнал ядра

4.4 Журналы аварийного режима

Журнал аварийного режима (см. Рисунок 31) является техническим, он не содержит обязательных полей, таких как идентификатор события, дата, результат.

В системе хранится всегда две разных копии аварийного журнала — *Текущий журнал* и *Предыдущий журнал*. Каждый из журналов расположен на своей вкладке.

Текущий журнал, в который вносятся все команды, выполняемые в командной строке, а также все команды, выполняемые в командной строке в аварийном режиме. По завершению аварийного режима текущий журнал переносится в предыдущий и очищается.

Предыдущий аварийный журнал, который содержит записи прошлой аварийной сессии от момента начала записи bash_history (выполнения команд из командной строки) до момента выхода из аварийного режима.

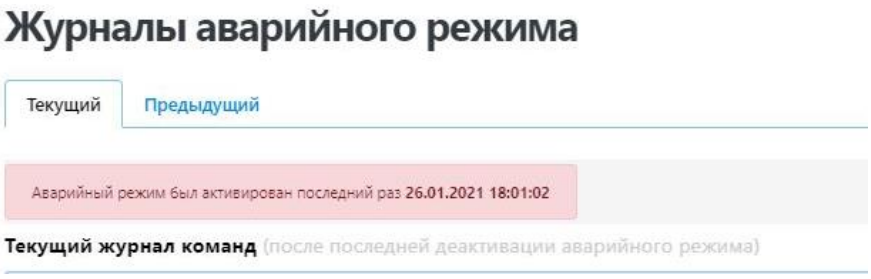


Рисунок 31. Журнал аварийного режима

4.5 Сеть

4.5.1 Сетевая статистика

Страница содержит список сетевых подключений по протоколам TCP и UDP, который представлен в табличном виде с со следующими полями:

- протокол;
- очереди приема;
- очереди отправки;
- локальный адрес;
- удаленный адрес;
- состояние;
- идентификатор процесса (PID).

На странице (см. Рисунок 32) реализованы следующие возможности управления контентом (по умолчанию все чекбоксы и радиокнопки, кроме *Соединения,* пустые):

- чекбокс *TCP* — на странице отображаются только соединения TCP;
- чекбокс *UDP* — на странице отображаются только соединения UDP;
- радиокнопка *Соединения* — при включении радиокнопки отображаются только данные, поле *Состояние* которых имеет статус *Установлено* (Established);
- радиокнопка *Ожидания соединения* — при включении радиокнопки отображаются только данные, поле *Состояние* которых имеет статус *Ожидание* (Listen);
- радиокнопка *Все* — при включении радиокнопки отображаются все данные;
- чекбокс *Символьные имена* — отображаются DNS имена узлов и порт соединения при наличии (по умолчанию отображаются IP-адреса узлов);
- *Обновить* — при нажатии кнопки происходит обновление данных на странице.

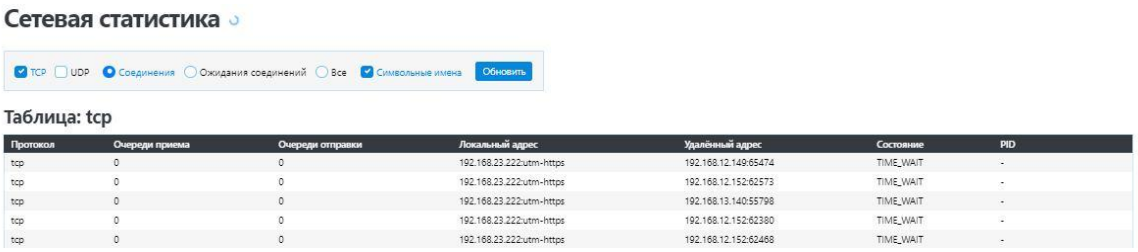


Рисунок 32. Сетевая статистика

4.5.2 Состояние межсетевого экрана

На данной странице (см. Рисунок 33) представлены таблицы IPTABLES (Filter, NAT, Mangle, Raw) по протоколам IPv4 и IPv6, а также реализованы кнопки управления: **Сбросить счетчики** и **Перезапустить межсетевой экран**.

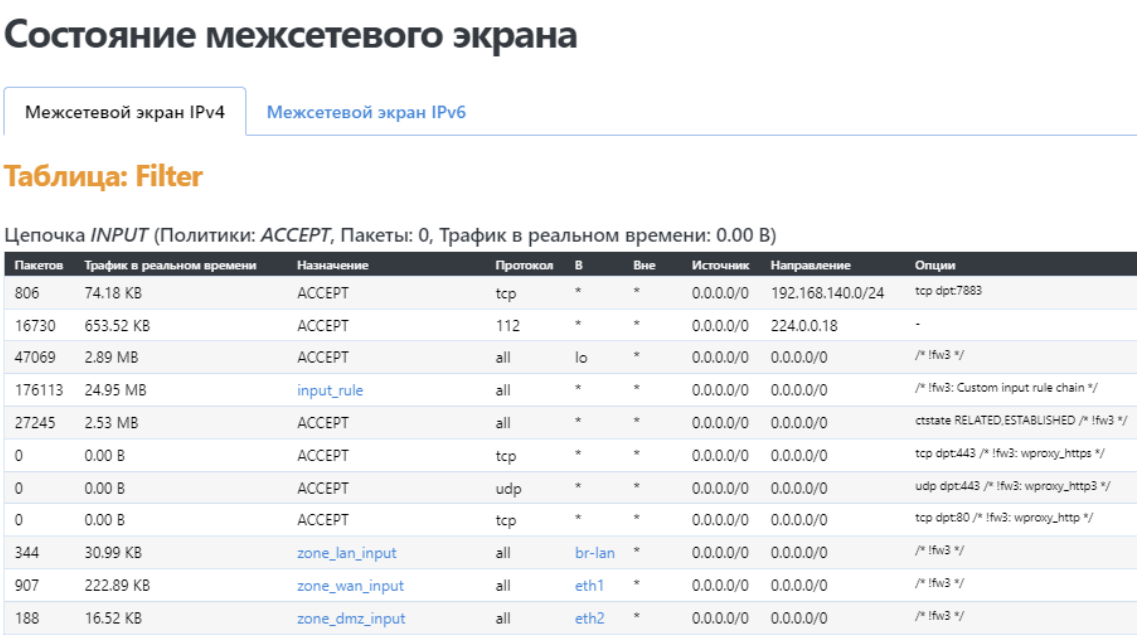


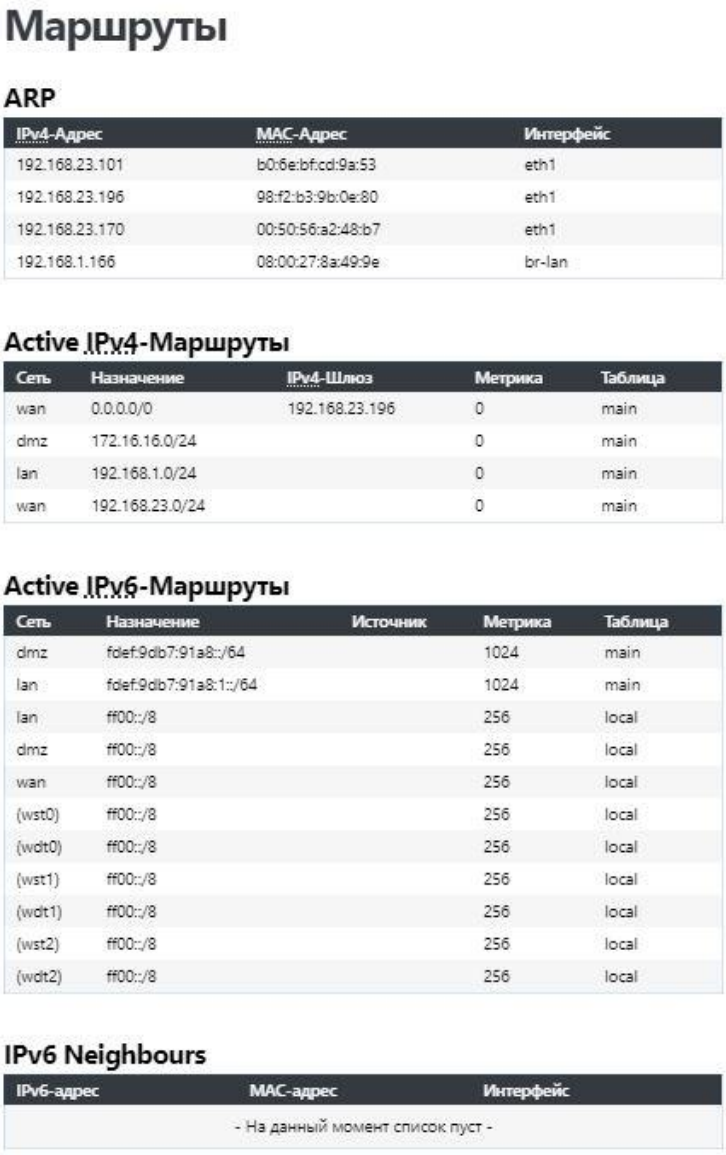
Рисунок 33. Состояние межсетевого экрана

4.5.3 Маршруты

На странице (см. Рисунок 34) представлены следующие правила маршрутизации в табличном виде:

- из таблицы ARP с полями *IPv4 Адрес, MAC Адрес и Интерфейс;*
- активные IPv4 маршруты с полями *Сеть, Назначение, IPv4 Шлюз, Метрика, Таблица;*
- активные IPv6 маршруты с полями *Сеть, Назначение, Источник, Метрика, Таблица;*

- протокол обнаружения соседей IPv6 (IPv6 Neighbours), с полями *IPv6 Адрес, MAC Адрес* и *Интерфейс.*



Маршруты

ARP

IPv4-Адрес	MAC-Адрес	Интерфейс
192.168.23.101	b0:6e:bf:cd:9a:53	eth1
192.168.23.196	98:f2:b3:9b:0e:80	eth1
192.168.23.170	00:50:56:a2:48:b7	eth1
192.168.1.166	08:00:27:8a:49:9e	br-lan

Active IPv4-Маршруты

Сеть	Назначение	IPv4-Шлюз	Метрика	Таблица
wan	0.0.0.0/0	192.168.23.196	0	main
dmz	172.16.16.0/24		0	main
lan	192.168.1.0/24		0	main
wan	192.168.23.0/24		0	main

Active IPv6-Маршруты

Сеть	Назначение	Источник	Метрика	Таблица
dmz	fdef:9db7:91a8::/64		1024	main
lan	fdef:9db7:91a8:1::/64		1024	main
lan	ff00::/8		256	local
dmz	ff00::/8		256	local
wan	ff00::/8		256	local
(wst0)	ff00::/8		256	local
(wdt0)	ff00::/8		256	local
(wst1)	ff00::/8		256	local
(wdt1)	ff00::/8		256	local
(wst2)	ff00::/8		256	local
(wdt2)	ff00::/8		256	local

IPv6 Neighbours

IPv6-адрес	MAC-адрес	Интерфейс
- На данный момент список пуст -		

Рисунок 34. Маршруты

4.6 Графики в реальном времени

Страница состоит из трех основных графиков:

- Загрузка системы.
- Трафик в реальном времени.
- Соединения.

На графике **Загрузка системы в реальном времени** (см. Рисунок 35) отображена динамика нагрузки системы в реальном времени. На графике отображается средняя и пиковая нагрузка системы за временной период: 1 минута, 5 минут, 15 минут. Рядом с временным промежутком отображается нагрузка на систему: в реальном времени, средняя, пиковая.

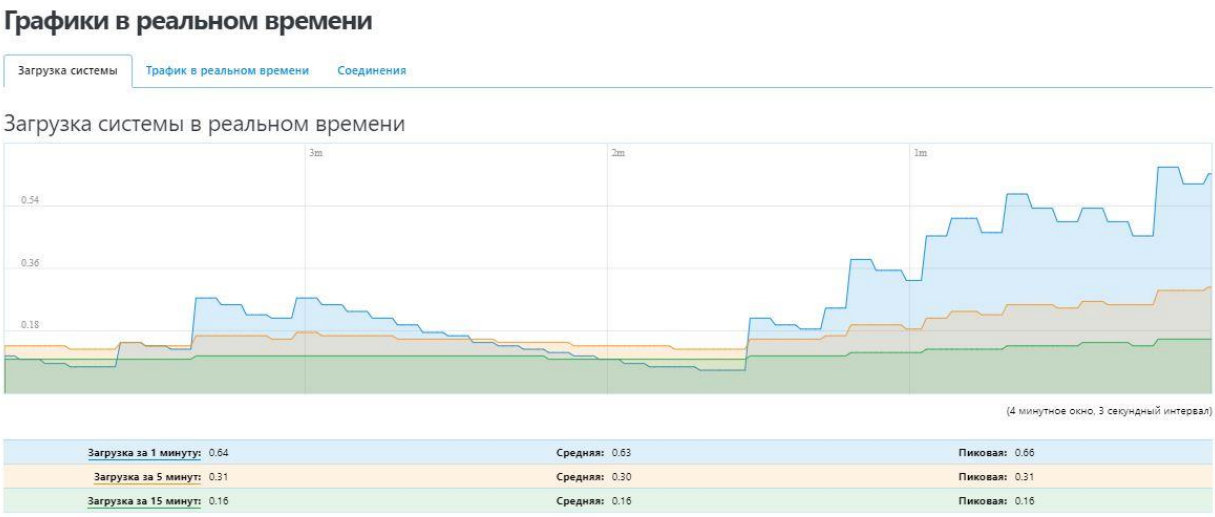


Рисунок 35. Загрузка в реальном времени

В графике **Трафик в реальном времени** (см. Рисунок 36) отображается информация о загрузке трафика сети. Трафик разделен на три вкладки по интерфейсам соединения (зоны LAN, WAN и DMZ). Подробное описание и настройка интерфейсов представлена в разделе 6.1 «Интерфейсы».

Под графиком отображена информация о загрузке входящих и исходящих данных в реальном времени, средней и пиковой загрузке. Скорость получения входящих и исходящих данных указана в килобитах и килобайтах.

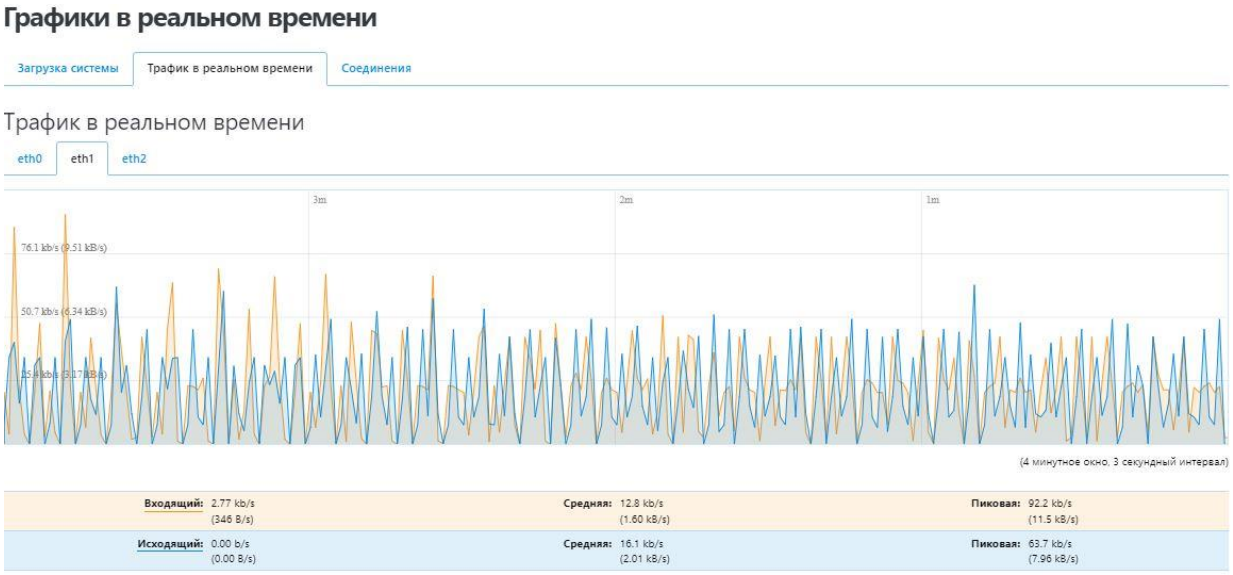


Рисунок 36. Трафик в реальном времени

График **Соединения в реальном времени** (см. Рисунок 37, Рисунок 38) содержит список всех активных на данный момент сетевых соединений по сетевым протоколам TCP, UDP и другим. На странице отображена подробная информация о сетевых соединениях: сеть, протокол, источник, направление, передача.

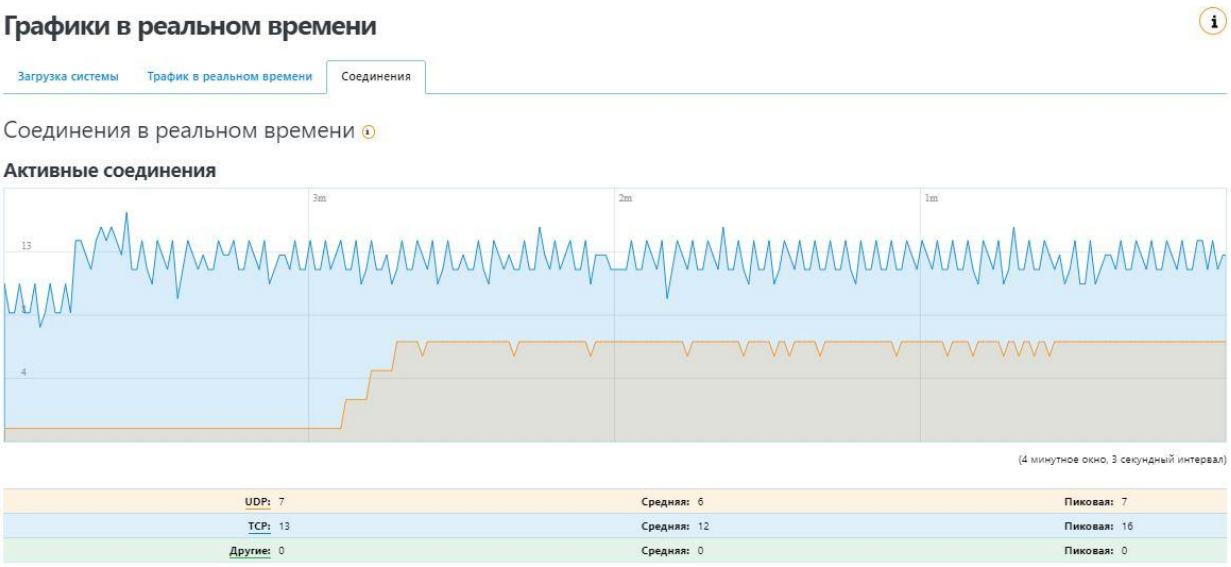


Рисунок 37. Соединения в реальном времени (график активных соединений)

Сеть	Протокол	Источник	Направление	Передача
IPV4	IGMP	192.168.77.1:0	224.0.0.1:0	101.39 KB (2884 Пакетов.)
IPV4	UDP	192.168.0.49:67	255.255.255.255:68	52.19 KB (150 Пакетов.)
IPV4	TCP	192.168.13.65:1040	192.168.23.222:7443	10.20 KB (22 Пакетов.)
IPV4	TCP	192.168.13.65:20933	192.168.23.222:7443	8.62 KB (23 Пакетов.)
IPV4	TCP	192.168.13.65:1049	192.168.23.222:7443	8.54 KB (21 Пакетов.)
IPV4	TCP	192.168.13.65:26280	192.168.23.222:7443	8.45 KB (23 Пакетов.)

Рисунок 38. Соединения в реальном времени (таблица активных соединений)

4.7 Процессы

На данной странице (см. Рисунок 39) представлен список всех имеющихся (запущенных) процессов, с данными об их состоянии, в том числе о потребляемых аппаратных ресурсах, а также с функциональной возможностью завершения и принудительного завершения каждого, отдельно взятого процесса.

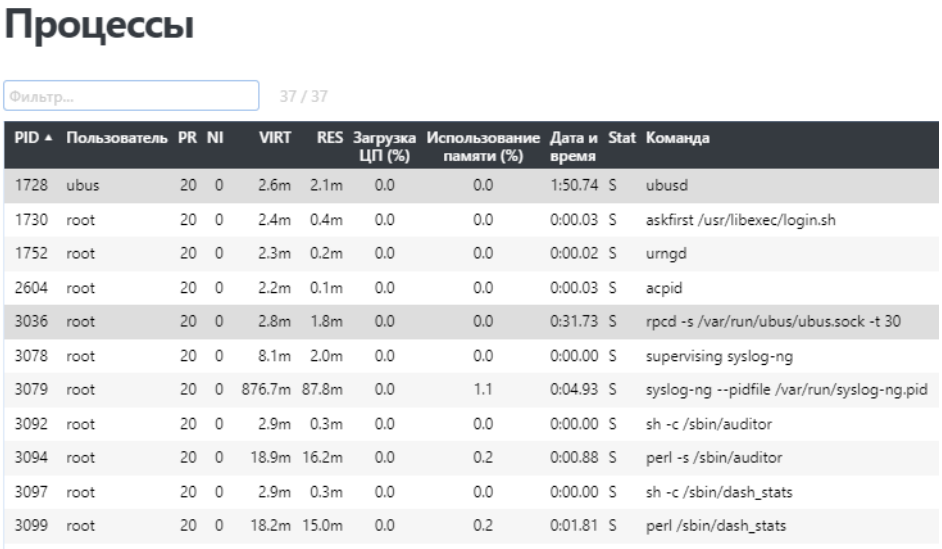


Рисунок 39. Процессы

4.8 Сведения о системе

На данной странице (см. Рисунок 40) представлены общие данные о системе, которые содержат:

- *Имя хоста **WAF Dallas Lock**.*

- *Модель устройства.* Наименование аппаратной платформы, на которую установлен **WAF Dallas Lock**. В случае использования виртуальной машины указывается виртуальная машина.
- *Система выпущена.* Информации о компании, которая разработала и выпустила данный продукт.
- *Версия прошивки.* Актуальная версия **WAF Dallas Lock**.
- *Версия ядра.* Версия операционной системы.
- *Номер лицензии.* Текущий номер лицензии продукта.
- *Код поддержки*. Уникальный идентификационный номер, предоставляемый клиентам для доступа к технической поддержке.
- *Дата и время.* Текущая дата и время.
- *Время работы.* Время беспрерывной работы.
- *Средняя нагрузка.* Данные в реальном времени о средней нагрузке на систему.

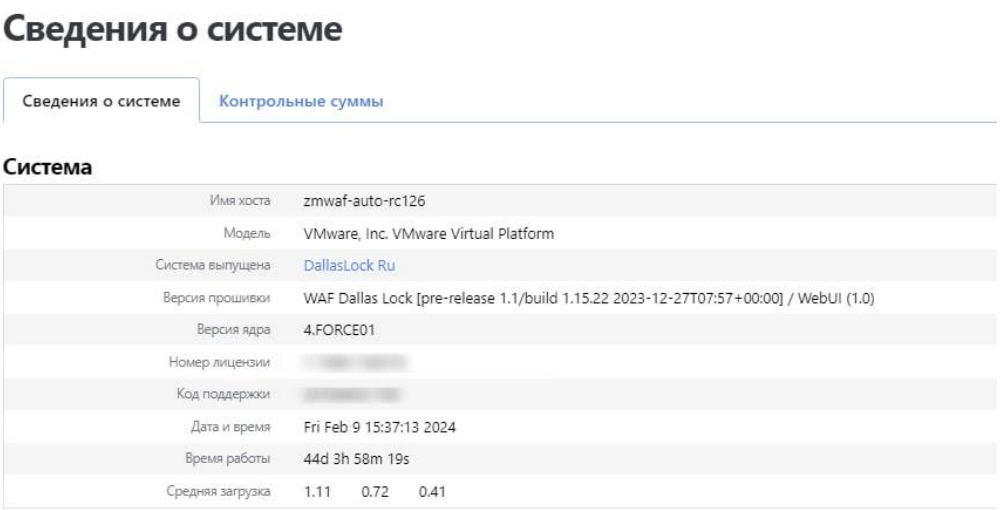


Рисунок 40. Система

4.8.1 Виджет «Оперативная память (RAM)»

Отображает в реальном времени размер свободного места в оперативной памяти и буферизацию (см. Рисунок 41).

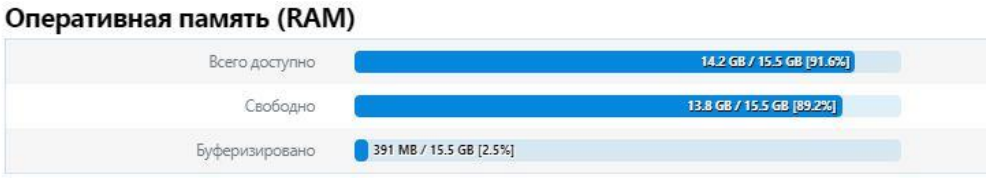


Рисунок 41. Оперативная память

4.8.2 Виджет «Использование диска»

Отображает в реальном времени общее свободное пространство на жестких дисках (см. Рисунок 42).

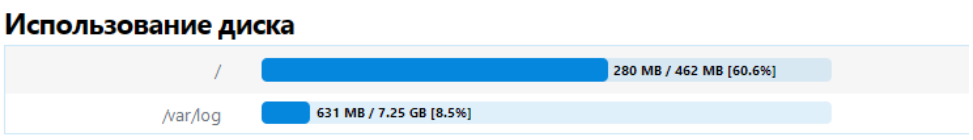


Рисунок 42. Использование диска

4.8.3 Сеть

Отображает данные о состоянии сети (см. Рисунок 43), содержащие данные о состоянии IPv4 WAN, IPv6 WAN и количестве активных соединений. Состояние WAN интерфейсов IPv4 и IPv6 содержит:

- тип соединения (статический или динамический);
- адрес соединения;
- маска сети;
- шлюз;
- предпочитаемый DNS-сервер;
- альтернативный DNS-сервер;
- подключен. Время непрерывного подключения интерфейса в реальном времени;
- активные соединения.

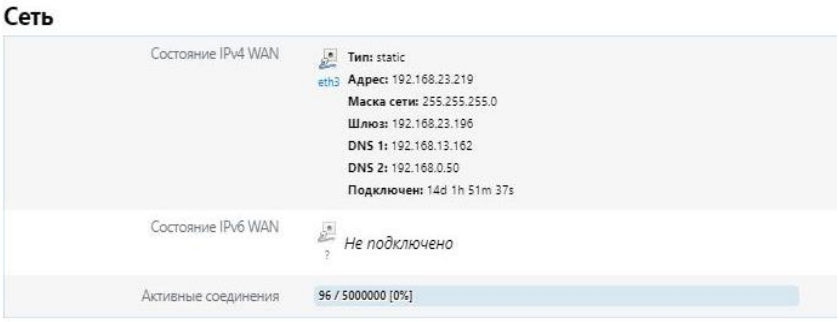
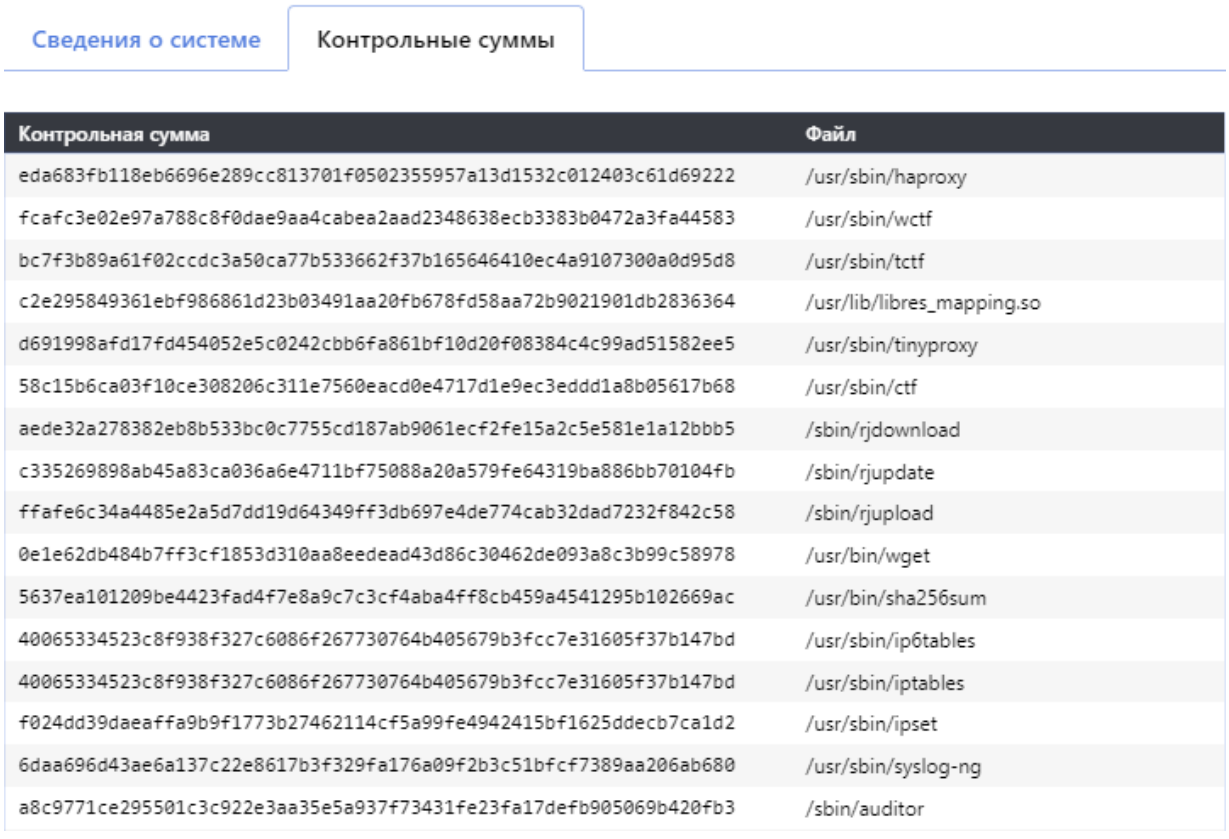


Рисунок 43. Сеть

4.8.4 Контрольные суммы

Информация о контрольных суммах исполняемых файлов **WAF Dallas Lock** отображается на вкладке *Контрольные суммы* страницы **Сведения о системе** (см. Рисунок 44). Расчет контрольных сумм осуществляется по алгоритму SHA-256.



Контрольная сумма	Файл
eda683fb118eb6696e289cc813701f0502355957a13d1532c012403c61d69222	/usr/sbin/haproxy
fcafc3e02e97a788c8f0dae9aa4cabea2aad2348638ecb3383b0472a3fa44583	/usr/sbin/wctf
bc7f3b89a61f02ccdc3a50ca77b533662f37b165646410ec4a9107300a0d95d8	/usr/sbin/tctf
c2e295849361ebf986861d23b03491aa20fb678fd58aa72b9021901db2836364	/usr/lib/libres_mapping.so
d691998afd17fd454052e5c0242cbb6fa861bf10d20f08384c4c99ad51582ee5	/usr/sbin/tinyproxy
58c15b6ca03f10ce308206c311e7560eacd0e4717d1e9ec3eddd1a8b05617b68	/usr/sbin/ctf
aede32a278382eb8b533bc0c7755cd187ab9061ecf2fe15a2c5e581e1a12bbb5	/sbin/rjdownload
c335269898ab45a83ca036a6e4711bf75088a20a579fe64319ba886bb70104fb	/sbin/rjupdate
ffafe6c34a4485e2a5d7dd19d64349ff3db697e4de774cab32dad7232f842c58	/sbin/rjupload
0e1e62db484b7ff3cf1853d310aa8eedead43d86c30462de093a8c3b99c58978	/usr/bin/wget
5637ea101209be4423fad4f7e8a9c7c3cf4aba4ff8cb459a4541295b102669ac	/usr/bin/sha256sum
40065334523c8f938f327c6086f267730764b405679b3fcc7e31605f37b147bd	/usr/sbin/ip6tables
40065334523c8f938f327c6086f267730764b405679b3fcc7e31605f37b147bd	/usr/sbin/iptables
f024dd39daeaffa9b9f1773b27462114cf5a99fe4942415bf1625ddecb7ca1d2	/usr/sbin/ipset
6daa696d43ae6a137c22e8617b3f329fa176a09f2b3c51bfcf7389aa206ab680	/usr/sbin/syslog-ng
a8c9771ce295501c3c922e3aa35e5a937f73431fe23fa17defb905069b420fb3	/sbin/auditor

Рисунок 44. Контрольные суммы

Для верификации программного обеспечения **WAF Dallas Lock** необходимо сверить отображающиеся значения со значениями контрольных сумм исполняемых файлов, представленных в Приложении А Формуляра ПФНА.501540.001 ФО.

5 НАСТРОЙКА WAF DALLAS LOCK

Основной инструмент администратора **WAF Dallas Lock** — раздел **Настройки**.

Для перехода к разделу необходимо в основном меню консоли выбрать **Настройки**. Вкладка **Настройки** не имеет своей страницы. При нажатии на нее происходит открытие списка меню второго уровня. Общий вид представлен ниже (см. Рисунок 45).

Данная вкладка содержит следующие страницы:

- WAF;
- UTM;
- Настройки модуля ЕЦУ;
- Общие;
- Пользователи;
- Сервисы;
- Управление сертификатами;
- Аварийный режим;
- GEO IP фильтр.

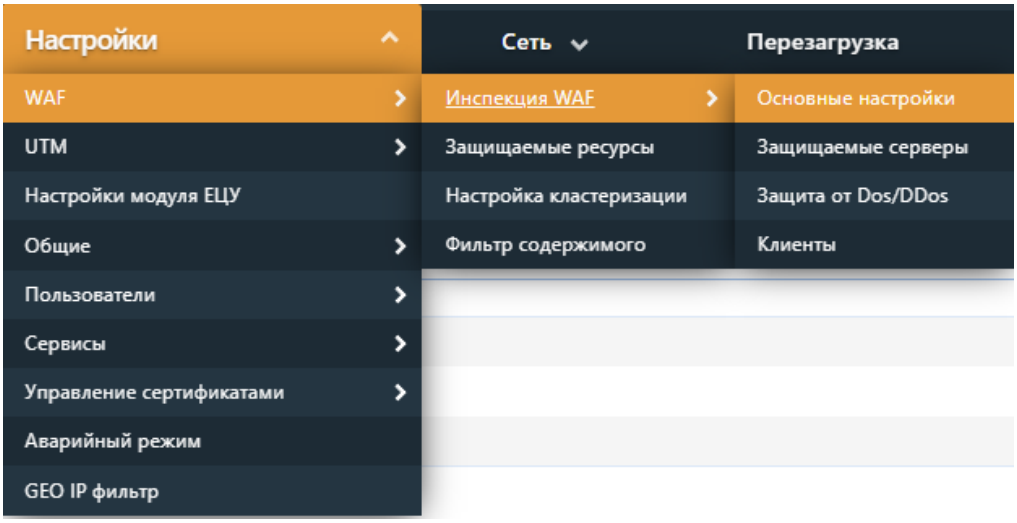


Рисунок 45. Меню Настройки

5.1 Настройки WAF

Для перехода к разделу настроек WAF необходимо в меню **Настройки** выбрать **WAF**. Произойдет открытие списка меню третьего уровня.

Данный раздел содержит следующие вкладки:

- Инспекция WAF;
- Защищаемые ресурсы;
- Настройка кластеризации;
- Фильтр содержимого.

5.1.1 Инспекция WAF

Для проверки работоспособности и корректности настроек WAF используется пункт настроек *Инспекция WAF*. Пункт делится на четыре уточняющие вкладки:

- Основные настройки;
- Защищаемые серверы;
- Защита от Dos/DDos;
- Клиенты.

На вкладке *Основные настройки* (см. Рисунок 46) предлагается включение или отключение процедуры инспекции и ее основные настройки, включающие количество очередей потоков обработки **WAF Dallas Lock**, быстрый анализ HTTP-ответов (при выборе данной опции обработка

ответов в CTF не происходит, анализ содержимого ответа сервера контент-фильтром не осуществляется).

В блоке **Точки входа** (см. Рисунок 46) доступны внутренние настройки соединений.

- *Включить HTTP*. При включенном чекбоксе разрешается HTTP-соединение, также становится доступными следующие настройки:
  - *HTTP порт*. Поле позволяет изменить порт HTTP (по умолчанию 80);
  - *HTTPS порт*. Поле позволяет изменить порт HTTPS (по умолчанию 443);
- *Доступная версия HTTP*. Выпадающий список позволяет выбрать версию протокола HTTP (значения: HTTP/1.1; HTTP/2; HTTP/3);
- *Keep-Alive или Close соединение.* Выпадающий список со следующими значениями*:*
  - *http-keep-alive*. Позволяет клиенту и серверу поддерживать открытое соединение после выполнения первого запроса. Последующие запросы могут быть отправлены без необходимости повторной установки соединения;
  - *http-close*. Означает, что после отправки запроса на сервер и получения ответа от него, соединение между клиентом и сервером будет закрыто.

Блок **Безопасное подключение** (см. Рисунок 46) включает следующие настройки:

- *Мин уровень протокола TLS* — задает ограничение на минимальное значение версии протокола TLS для браузера клиента. Значение по умолчанию — TLS v1.2;
- *Включить HSTS* — настройка активирует механизм *Strict Transport Security* (HSTS). Данный механизм обеспечивает безопасное соединение, требуя от клиента использование протокола HTTPS вместо HTTP. При первом обращении клиента к защищаемому ресурсу сервер возвращает заголовок *Strict Transport Security*, браузер клиента запоминает указанную информацию и все дальнейшие попытки доступа к сайту по протоколу HTTP будут автоматически преобразовываться в HTTPS, пока не истечет период времени, указанный в опции *Max-Age*;
- *Опция Max-Age* — время, указанное в секундах, в течение которого доступ к сайту должен осуществляться только по протоколу HTTPS. Значение по умолчанию — 16000000s.

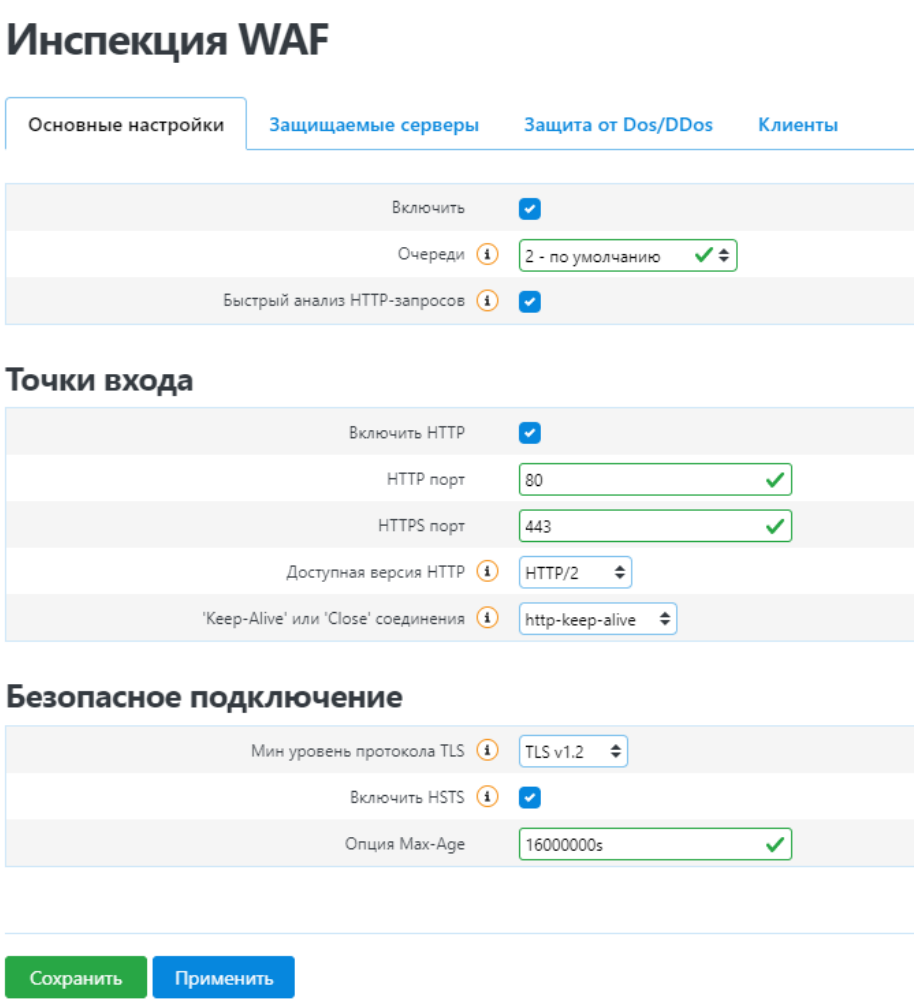


Рисунок 46. Инспекция WAF. Основные настройки

На вкладке *Защищаемые серверы* (см. Рисунок 47) отображается список объектов, которые находятся под защитой **WAF Dallas Lock**. В любой момент можно внести новые объекты, либо изменить существующие, согласно разделу 2.7 Добавление защищаемого ресурса.

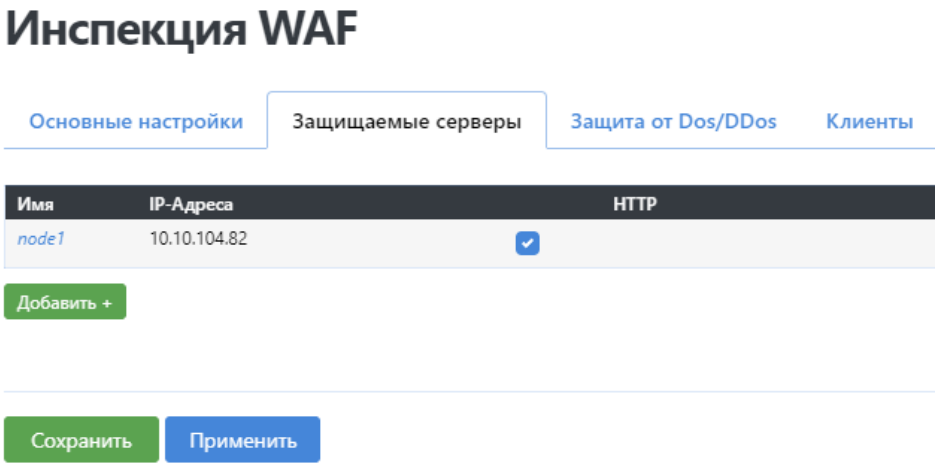


Рисунок 47. Инспекция WAF. Защищаемые серверы

Вкладка *Защищаемые серверы* (см. Рисунок 48) позволяет произвести настройки для сервера, который вводится или уже введен под защиту **WAF Dallas Lock**. Содержит следующие настройки:

- *Имя.* Поле не доступно для редактирования. Отображается имя защищаемого сервера «node*», где * — порядковый номер.

- *Тип сервера.* Выпадающий список, позволяющий назначить основной сервер или выбрать тип дополнительного сервера. Возможные значения:
    - *Основной. З*начение определяет основной сервер для защищаемого ресурса. Обязательно должен быть назначен один основной сервер у каждого защищаемого ресурса.
    - *WebSocket*. Значение определяет дополнительный выделенный сервер с поддержкой wss/ws. Соединение между клиентом и сервером остается активным до тех пор, пока оно не будет разорвано любой из сторон.
    - *По префиксу.* Значение определяет дополнительный сервер. При выборе данного значение доступно поле *Префикс в URI.* Поле задает дополнительную часть URL-адреса, которая появляется между доменным именем защищаемого ресурса (порт) и фрагментом URL-адреса страницы.
- *IP-Адреса.* Поля задают IP-адреса защищаемого сервера (IPv4).
- *Тип распределения.* Выбор алгоритма, распределяющего нагрузку между серверами. Возможные значения:
    - *roundrobin.* Запросы отправляются к серверам по очереди, в зависимости от их загрузки.
    - *static-rr.* Статический тип распределения нагрузки. Алгоритм аналогичен *round-robin,* но при изменении нагрузки на один из серверов очередность оправки запросов не изменится.
    - *leastconn:* Запрос отправляется к серверу с наименьшим количеством открытых соединений.
    - *first.* Запрос отправляются первому доступному серверу.
    - *source. З*апросы с одного IP-адреса всегда отправляются на один и тот же сервер.
- *Redispatch.* Чекбокс включает перераспределение запросов после обрыва соединения с каким-либо сервером.
- *HTTP/WS.* Чекбокс включает незашифрованное соединение. По умолчанию выключен. Если чекбокс выключен доступны следующие поля:
    - *Доступная версия HTTP.* Выпадающий список позволяет выбрать версию протокола HTTP, используемую на сервере (значения: HTTP/1.1; HTTP/2; HTTP/3);
    - *CA-сертификат.* Корневой сертификат сервера. При отсутствии будет сохранен после первого подключения. Загружаемый сертификат должен совпадать с сертификатом на сервере. В случае если сертификаты не совпадут, то при первом подключении к серверу будет выдана соответствующая ошибка.
    - *Сертификат двусторонней аутентификации.* Поле доступно после загрузки CA-сертификата. Позволяет использовать ключи веб-интерфейса для сертификата клиента при подключении к защищаемому серверу.
- *Защита CSRF.* Чекбокс включает защиту защищаемого сервера от атаки CSRF (cross-site request forgery, подделка межсайтовых запросов). При выключенной *Защите CSRF* доступна настройка:
    - *Cache.* Чекбокс включает cache для сервера на **WAF Dallas Lock**, что позволяет снизить количество запросов к серверу.
- *Keep-Alive or Close connection.* Выпадающий список с позволяющий выбрать поддержку открытого соединения с защищаемым сервером. Возможные значения:
    - *http-keep-alive.* Режим постоянного HTTP-соединения.
    - *http-server-close.* HTTP-соединение закрывается на стороне сервера. При этом на стороне клиента сохраняется возможность поддержки постоянного HTTP-соединения.
    - *httpclose.* HTTP-соединение закрывается на стороне клиента или сервера, в зависимости от того, где установлена эта опция.
    - *http-pretend-keepalive. И*митация поддержки активного соединения (keep-alive) с сервером, несмотря на то, что на самом деле соединение будет закрыто после отправки ответа.
- *Расширенные настройки.* Чексбокс включает дополнительные параметры и делает доступными настройки:
    - *Тайм-аут сервера.* Устанавливает максимальное время ожидания отправки данных

серверу.

- *Тайм-аут подключений.* Задает максимальное время ожидания успешного подключения к серверу.
- *Тайм-аут состояния.* Задает дополнительный тайм-аут сервера после установки соединения.
- *Check server.* Чекбокс включает проверку на стороне сервера.
- *Forward-For.* Чекбокс включает добавление заголовка X-Forwarded-For в запросы, отправляемые на сервер.

- *Описание.* Поле добавляет произвольное описание защищаемого сервера. Описание будет отображаться при выборе защищаемых серверов в разделе 5.1.2 Защищаемые ресурсы. Если поле *Описание* не заполнено, то будет отображаться *Имя* сервера.

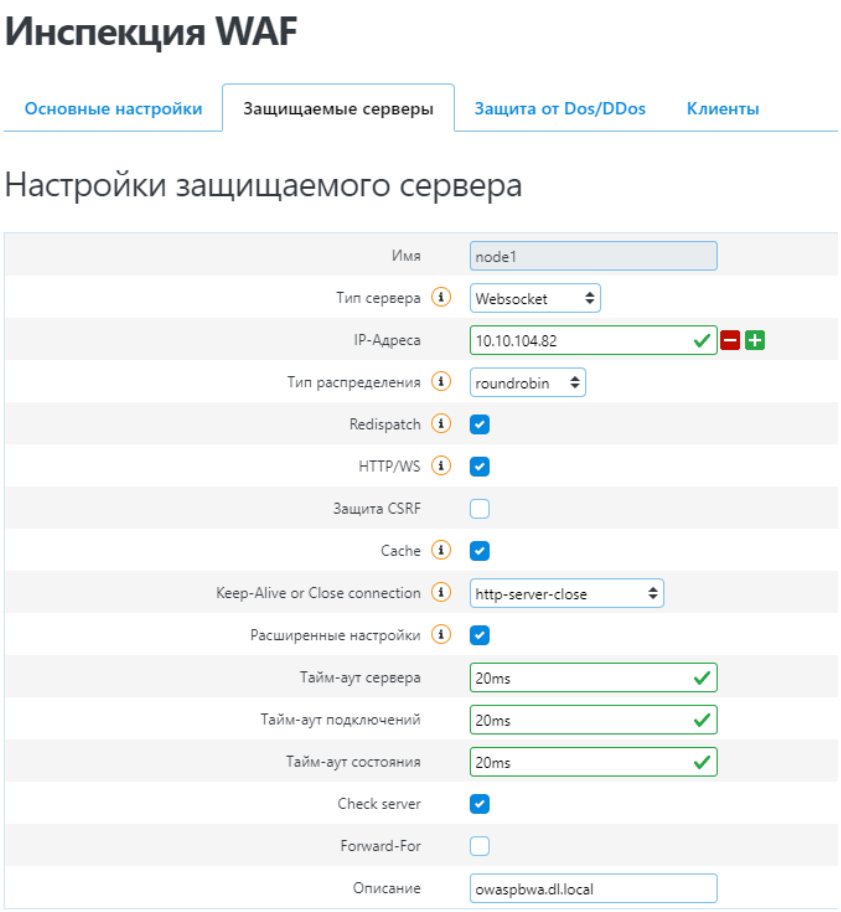


Рисунок 48. Настройки защищаемого сервера

На вкладке *Защита от Dos/DDos* (см. Рисунок 49) отображается два блока настроек, предназначенных для снижения влияния DoS/DDoS атак на защищаемые ресурсы.
Блок настроек **Защита от Slowloris** включает в себя следующие поля настроек:

- *Количество открытых соединений.* Задает максимальное количество открытых соединений на 1 порт. По умолчанию значение 32000;
- *Переход в усиленную защиту при достижении.* В данном режиме **WAF Dallas Lock** не принимает новых подключений, также вводит дополнительную фильтрацию подозрительных пакетов. По умолчанию 80 процентов;
- *Тайм-аут HTTP запросов.* Задает максимально допустимое время ожидания завершения HTTP запросов. По умолчанию 5 секунд;
- *Тайм-аут для клиента.* Задает максимальное время бездействия на стороне клиента. По умолчанию 5 секунд;
- *Тайм-аут для HTTP-туннелей.* Задает максимальное время бездействия для HTTP-туннелей на стороне клиента и сервера. По умолчанию 1 час.

Блок настроек **Предотвращение DOS-атак** представлена следующими настройками:

- *Максимальное число клиентов без client id.* Применяется для защиты от ботов. Задает ограничение количества клиентов без client id, отправляющих запросы с одного IP-адреса. Поле *«за»* задает временной интервал (диапазон значений от 10s до 100s, значение по умолчанию 10 секунд);
- *Включить ограничение числа запросов.* При активации чекбокса станут доступны следующие настройки HTTP запросов:
  - *Максимальное число запросов от одного клиента.* Задает ограничение числа запросов защищаемого ресурса от одного клиента. Применяется для защиты от атак scanning, HTTP-flood. Поле *«за»* задает временной интервал;
  - *Максимальное число запросов с ошибками.* Задает ограничение числа запросов с ошибками на защищаемом ресурсе. Поле *«за»* задает временной интервал;

При заполнении полей: *Тайм-аут HTTP запросов*, *Тайм-аут для клиента*, *Тайм-аут для HTTP туннелей*, *за (Максимальное число запросов от одного клиента)*, *за (Максимальное число запросов с ошибками)* используются суффиксы «s» — для указания секунд, «m» — минут, «h» — часов, «d» — дней.

При нажатии кнопки **Сохранить** происходит сохранение введенных настроек в форме веб-интерфейса. При нажатии кнопки **Применить** происходит запись введенных настроек в соответствующие config-файлы. Нажатие кнопки **Сброс** приводит к удалению введенных данных, которые не были сохранены (записаны в config-файлы) ранее.

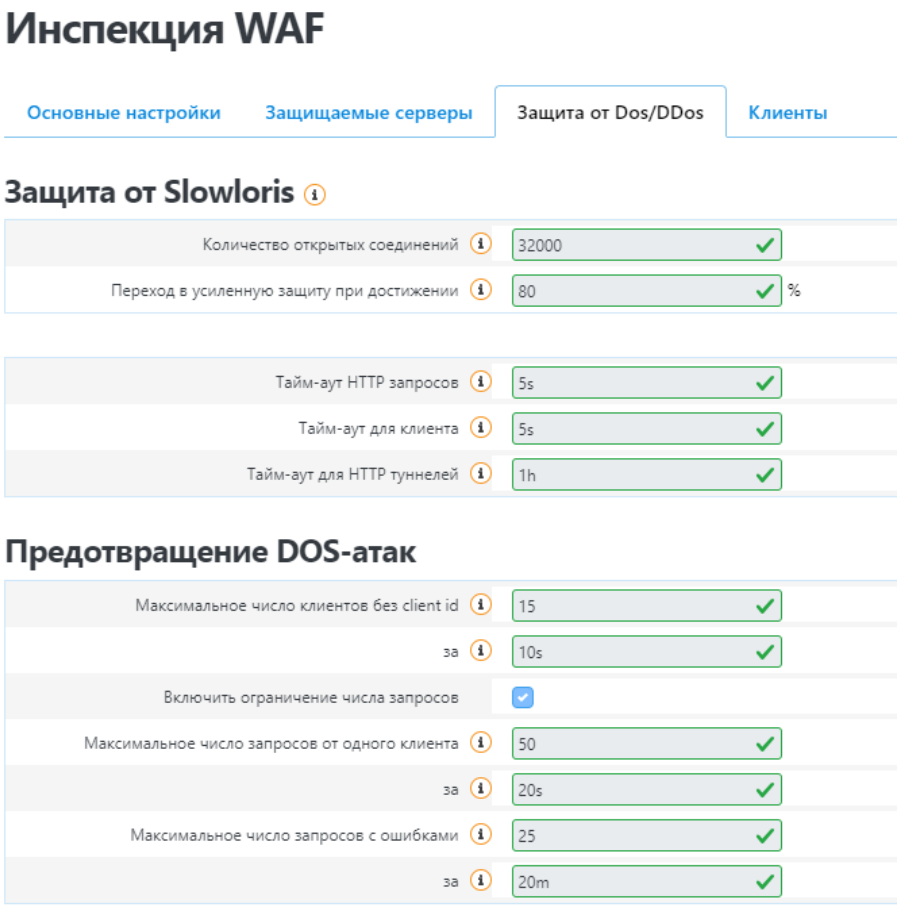


Рисунок 49. Инспекция WAF. Защита от Dos/DDos

На странице *Клиенты* (см. Рисунок 50) отображаются указанные корневые сертификаты Удостоверяющих центров (УЦ), а также списки отозванных сертификатов по каждому УЦ. Их можно добавить либо с помощью файла, либо указать URL источника.

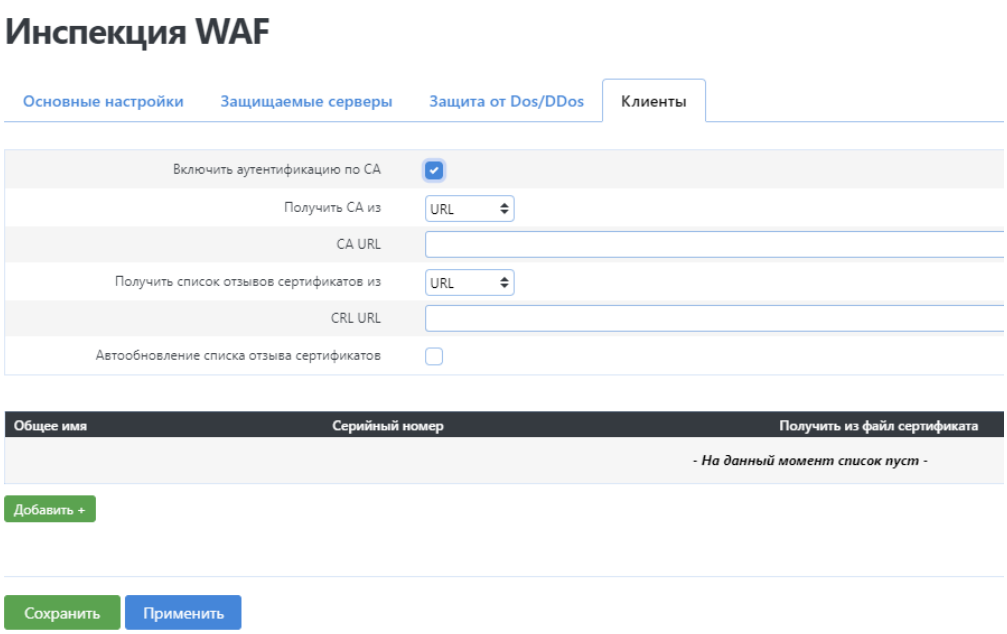


Рисунок 50. Инспекция WAF. Клиенты

Для осуществления инспекции трафика необходим как минимум один УЦ (желательно аккредитованный). Для каждого участника взаимодействия в рамках инспекции (**WAF Dallas Lock**, как устройство, выполняющее инспекцию трафика, и инспектируемых серверов/хостов) необходимо выполнить следующие действия:

- На УЦ необходимо сгенерировать пару открытый/закрытый ключ. Пример генерации на ОС Windows с использованием OpenSSL представлен в разделе

> При резервном копировании конфигурации **WAF Dallas Lock** сохраненные ключи аутентификации SSH не сохраняются и требуют повторного импорта на **WAF Dallas Lock.**

- 5.4.2.2 Web-интерфейс.Аутентификация по сертификату.
- На каждой инспектируемой станции необходимо установить следующие ключи: корневой сертификат УЦ, открытый ключ **WAF Dallas Lock** и пару открытый/закрытый ключ для инспектируемого сервера/хоста.

Пара открытый/закрытый ключ для **WAF Dallas Lock** добавляется во вкладке *Защищаемые ресурсы* согласно разделу 5.1.2 Защищаемые ресурсы. Пошаговый пример настройки представлен в разделе 5.1.5 Настройка инспекции защищаемого узла.

Для добавления сертификатов УЦ можно выбрать один из возможных способов в случае выбора:

- *URL* — будет предложена строчка «CA URL» для указания ссылки (URL) на сертификат;
- *Файл* — будет предложена строчка «CA File» для указания пути к файлу.

Аналогичная настройка необходима для указания источника списка отозванных сертификатов соответствующего УЦ. Также существует возможность автоматического обновления списка отозванных сертификатов УЦ, при условии выбора указания URL на необходимый список.

5.1.2 Защищаемые ресурсы

Настройка **Защищаемые ресурсы** (см. Рисунок 51) позволяет добавить новые объекты защиты (домены для инспекции), а также выбрать профиль приложения, развернутого на этом объекте, и указать требуемую политику контента для развернутого приложения.

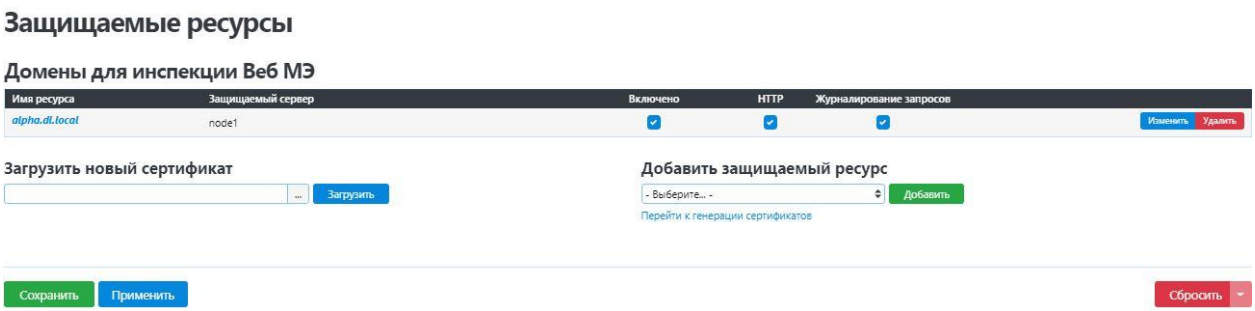


Рисунок 51. Добавление и редактирование защищаемого ресурса

После добавления сертификата возможно внести дополнительные настройки для нового домена, указав защищаемый сервер, на котором он располагается, а также настроив возможность работы с HTTP-трафиком, если чекбокс *HTTP* выключен, то используется HTTPS соединение. Затем, необходимо включить защищаемый ресурс в работу **WAF Dallas Lock**, поставив чекбокс в строке *Включено* (см. Рисунок 52).

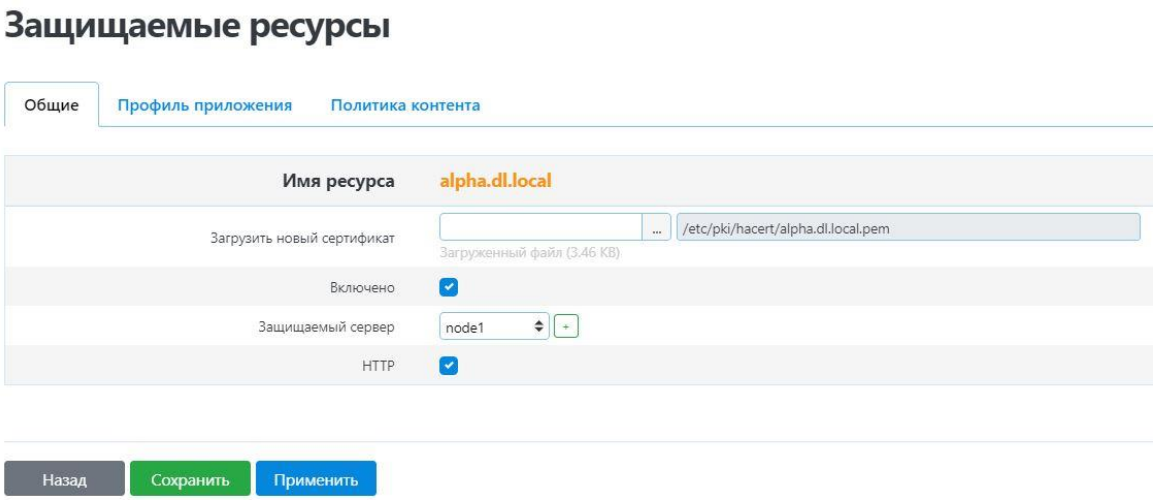


Рисунок 52. Общие настройки

Далее необходимо перейти на вкладку *Профиль приложения* (см. Рисунок 53) для указания опций профиля рассматриваемого объекта.

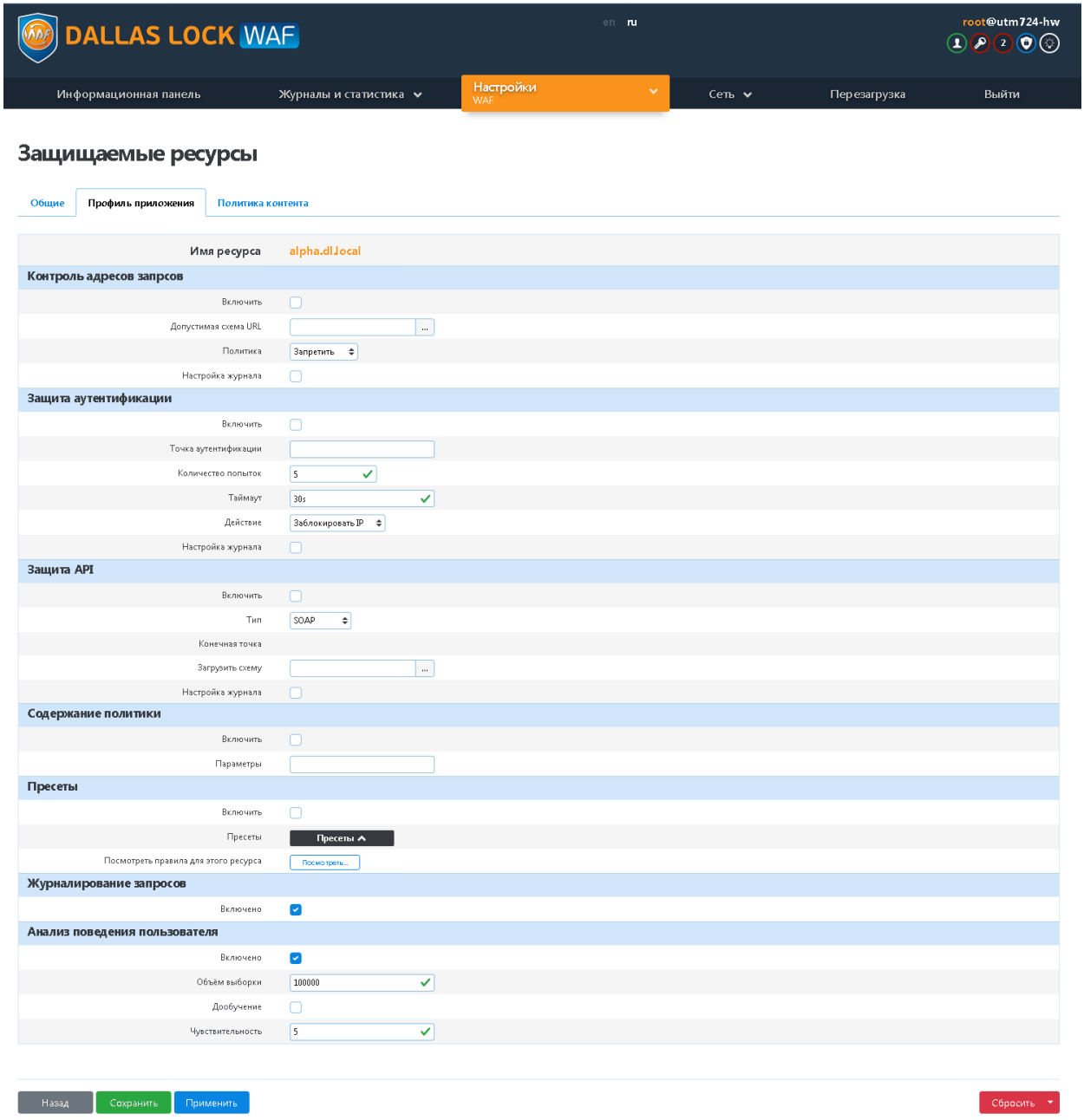


Рисунок 53. Настройки правил WAF. Защищаемые ресурсы

Здесь можно задать параметры безопасности для рассматриваемого объекта.

Пункт **Контроль адресов запросов** необходим для проверки схемы запросов к домену. Для этого необходимо загрузить готовую схему, указать политику Разрешено/Запрещено для представленной схемы запросов и включить данный параметр, установив чекбокс напротив *Включено*. Функция *Допустимая схема URL* обеспечивает загрузку файла схемы допустимых URL. Параметр *Настройка журнала* необходима для редактирования и настройки выходных данных в журнале.

Пункт **Защита аутентификации** необходим для настройки авторизации на защищаемом домене. Указываются точки аутентификации, откуда возможно подключение к домену, количество неуспешных попыток входа, время таймаута, а также, на выбор, действие, которое необходимо совершить при превышении неуспешных попыток авторизации в домене: *Заблокировать IP*, *Заблокировать ID*. Параметр *Настройка журнала* необходим для редактирования и настройки выходных данных в журнале. Включить данный параметр возможно, установив чекбокс напротив *Включено*.

Пункт **Защита API** необходим для выбора схемы вызова процедур, направленных на защиту API клиента. Возможность выбора типа загружаемой схемы: *SOAP, XML-RPC*. Функция *Загрузить схему* обеспечивает загрузку внешнего файла схемы веб-приложения. Параметр *Настройка журнала*

необходим для редактирования и настройки выходных данных в журнале. Включить данный параметр возможно, установив чекбокс напротив *Включено*.

Пункт **Содержание политики** необходим для указания дополнительных параметров политики безопасности. И включить данный параметр возможно, установив чекбокс напротив *Включено*.

Пункт **Пресеты** необходим для выбора пресетов правил **WAF Dallas Lock** для настраиваемого приложения. Возможно группировать не только предоставляемые пресеты, но и те, что были созданы администратором (пользовательские пресеты). Включить данный параметр возможно, установив чекбокс напротив *Включено*.

Пункт **Журналирование запросов** необходим для включения/отключения режима журналирования поступающих запросов на защищаемый ресурс. Включить данный параметр возможно, установив чекбокс напротив *Включено*.

Пункт **Анализ поведения пользователя** необходим для настройки срабатывания политики безопасности, следящей за операциями, совершаемыми пользователями. Возможно задать объем выборки, в границах которой будут рассмотрены совершаемые операции пользователя. Также есть возможность выбрать операцию *Дообучение* для задания примеров нестандартного поведения пользователя, указав периодичность выборки образца для политики. Для итоговой политики также необходимо указать параметр *Чувствительность* для задания коэффициента реагирования на события. Включить данный параметр возможно, установив чекбокс напротив *Включено*.

После указания параметров профиля приложения, в случае необходимости, нужно указать политики контента для настраиваемого приложения по категориям (см. Рисунок 54).

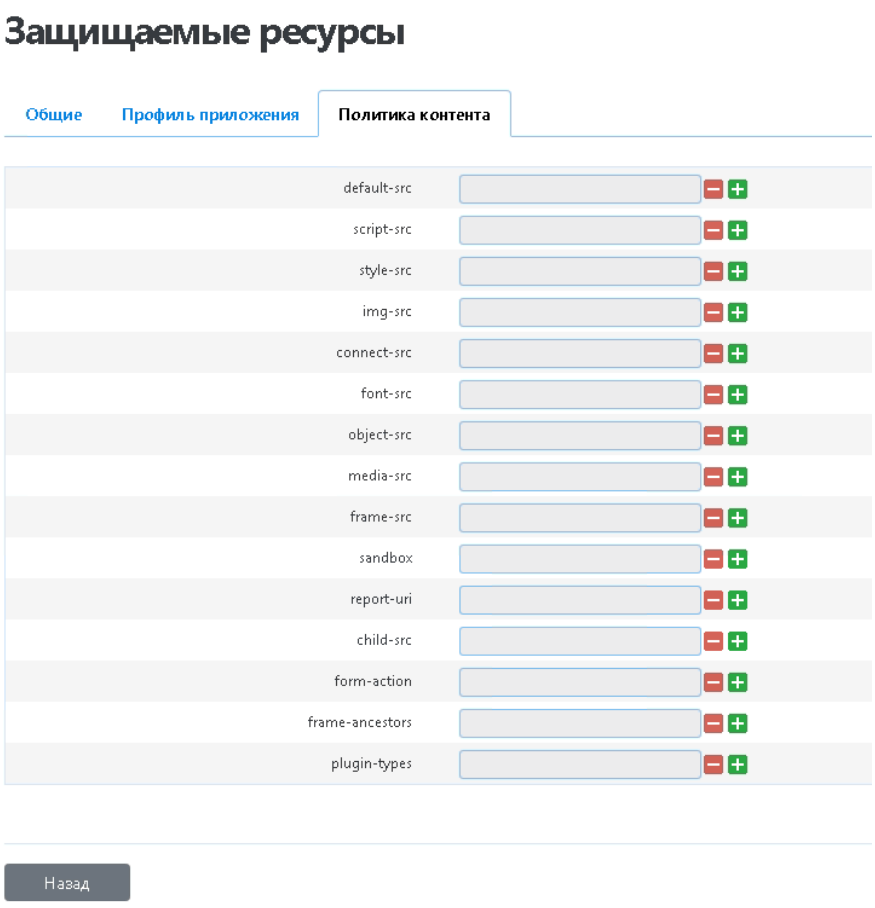


Рисунок 54. Настройки правил WAF. Защищаемые ресурсы

5.1.3 Настройка кластеризации

В рамках **WAF Dallas Lock** реализована функциональная возможность работы в режиме отказоустойчивого кластера по схеме *Active-Passive* и миграции конфигурационных настроек между несколькими машинами. В каждый момент времени только устройство с ролью *Master* обрабатывает весь трафик, связанный с защищаемыми ресурсами. Резервные устройства в подчинении постоянно синхронизируют свое состояние с мастер-устройством.

Необходимо в **Настройках** перейти в раздел **WAF** и выбрать пункт *Настройка кластеризации* (см. Рисунок 55).

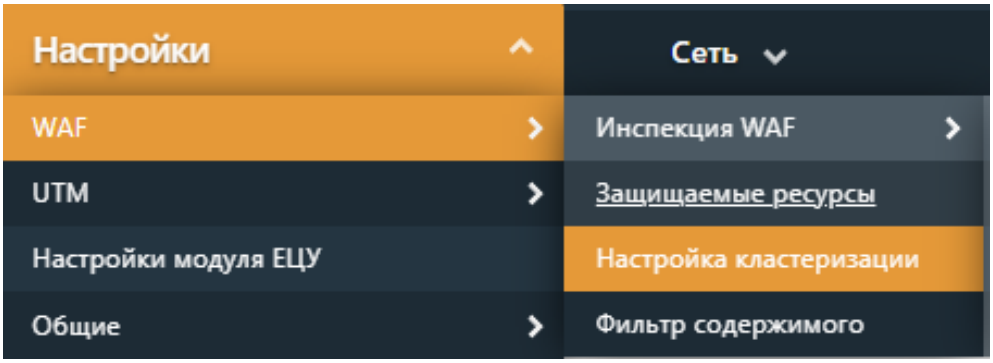


Рисунок 55. Пункт Настройка кластеризации в меню

Чтобы войти в уже существующий кластер, необходимо нажать на ссылку Перейти к отключению WAF и отключить WAF на открывшейся странице (см.Рисунок 56).
Чтобы создать новый кластер установите галочку в соответствующем чекбоксе (см. Рисунок 56), после чего для редактирования будут доступны два блока:

- Настройки виртуального интерфейса для WAF, где необходимо задать виртуальный IP для интерфейса WAN.
- Настройки виртуального интерфейса для репликаций, где указываем виртуальный IP для интерфейса LAN.

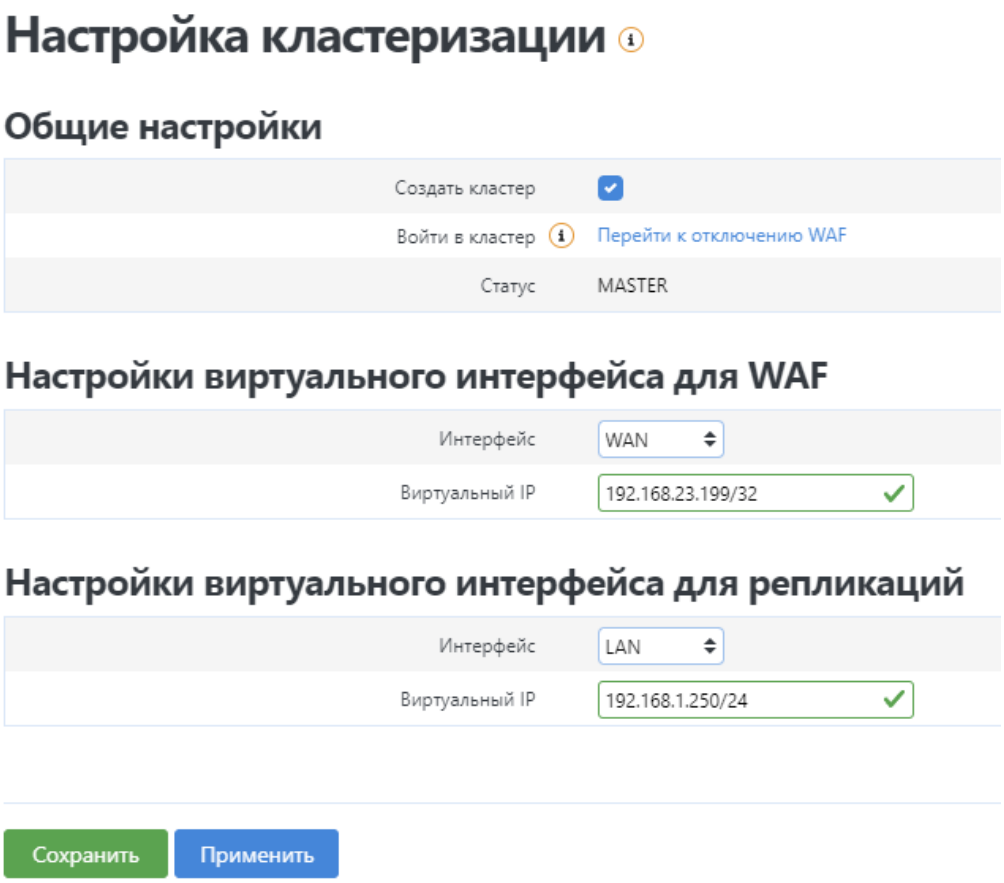


Рисунок 56. Создание нового кластера

После чего необходимо скачать конфигурационные настройки на жесткий диск для загрузки их в другой узел при добавлении его в кластер.

В блоке **Список узлов** отобразятся узлы, участвующие в кластере: *Master-узел* и *backup-устройства* (см. Рисунок 57). Здесь же через нажатие соответствующих кнопок можно вывести узел из кластера или сделать резервное устройство Мастером.

Рисунок 57. Список узлов

В случае, если *Master* выходит из строя, его подменяет одно из резервных устройств, которому переходит статус *Master*. Новый мастер способен прозрачно подхватить и продолжить обработку сетевых потоков. Если в **Общих настройках** включен режим вытеснения (см. Рисунок 58), изначальный мастер-узел возвращает себе все права, как только его работа возобновляется.

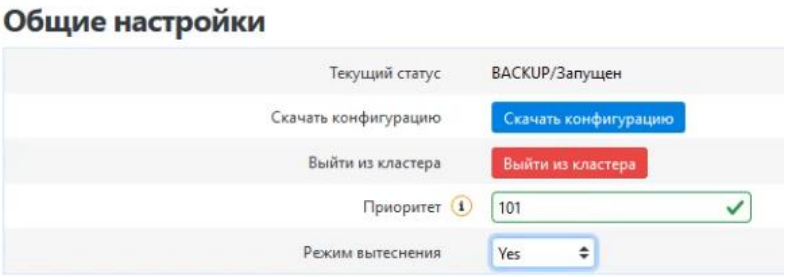


Рисунок 58. Режим вытеснения

5.1.4 Фильтр содержимого

Более детализированное отображение созданных правил для WAF Dallas Lock на вкладке **Фильтр содержимого.** Здесь же в разделе **WAF** есть возможность вручную включить/отключить работу WAF, просмотреть количество активных правил, общее количество настроенных правил, количество правил из Базы решающих правил, а также отфильтровать правила по тегам: *Пресет, Имя ресурса, IP*; а также по произвольному фильтру (по названию или номеру правила) (см. Рисунок 59).

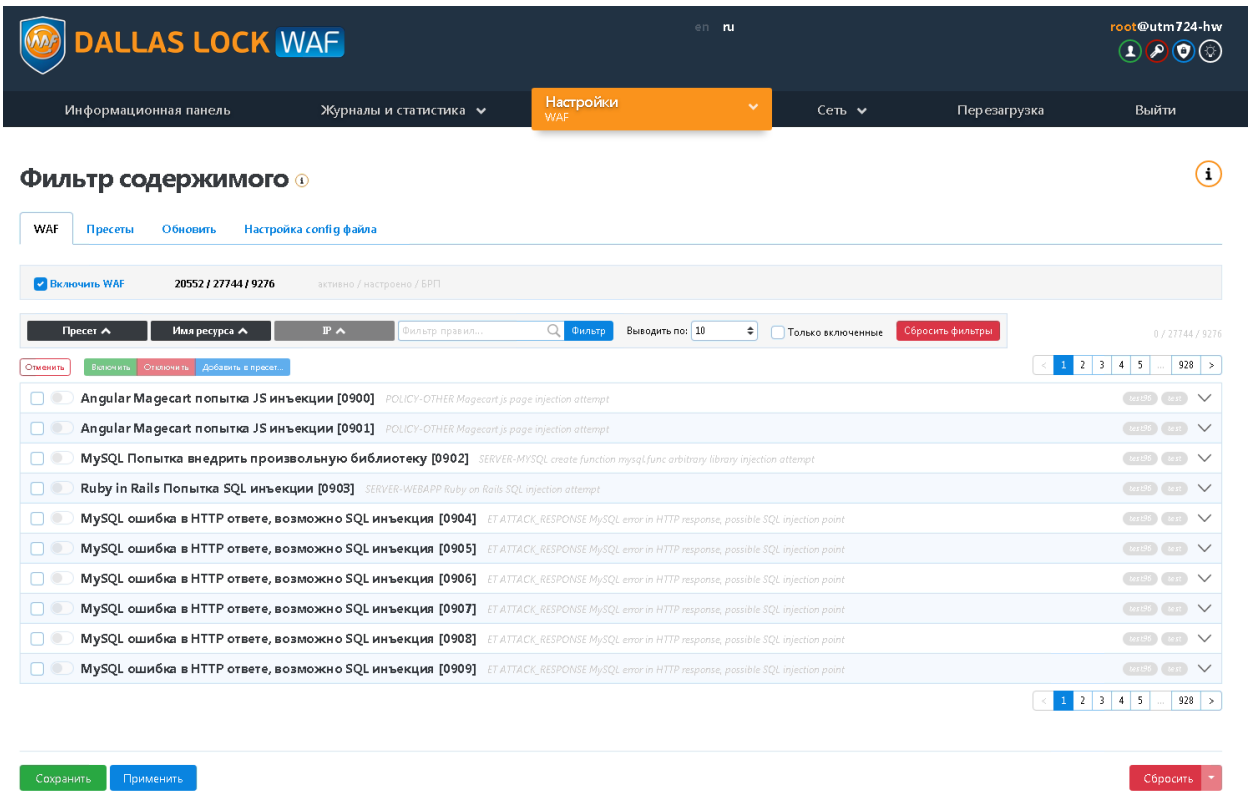


Рисунок 59. Настройка правил WAF. Фильтр содержимого. WAF

Существует возможность изменить правила под свою инфраструктуру, задав уточняющие данные, либо включить/отключить составляющие политики для правила (см. Рисунок 60, Рисунок 61).

Правила пресета *Forbidden Data* и *Forbidden Methods* являются сервисными пресетами. Их включение приводит к коду ответа 403 для защищаемого узла со всех адресов.

Рисунок 60. Настройка правил WAF. Фильтр содержимого. WAF

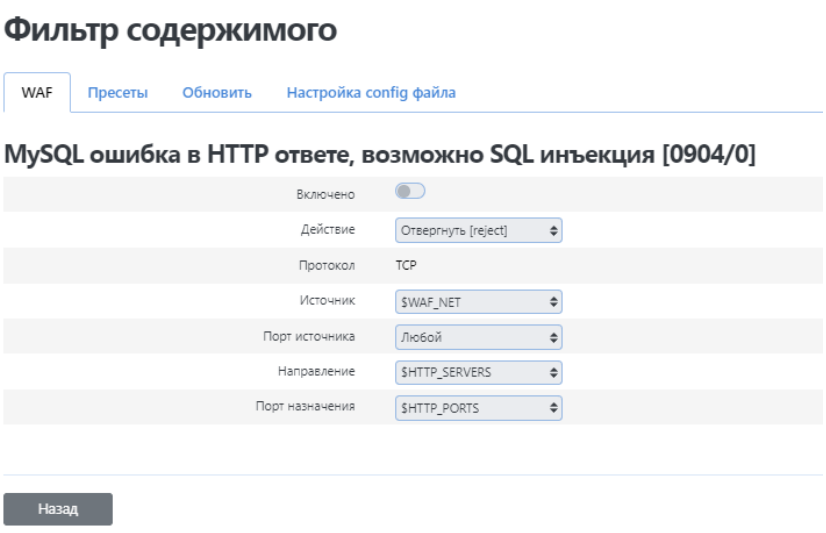


Рисунок 61. Настройка правил WAF. Фильтр содержимого. WAF

Вкладка *Пресеты* служит для группировки и отображения характеристик правил для приложений. Возможно группировать не только предоставляемые пресеты, но и те, что были созданы администратором (пользовательские пресеты) (см. Рисунок 62).

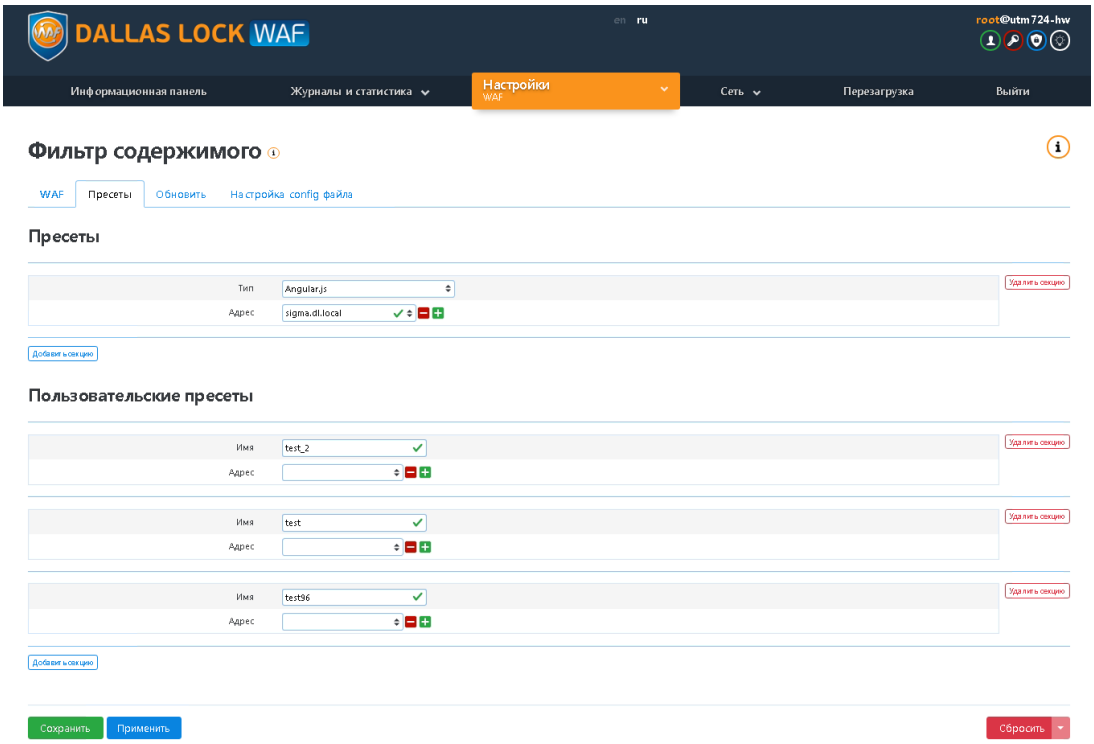


Рисунок 62. Настройка правил WAF. Фильтр содержимого. Пресеты

Вкладка **Обновить** служит для задания настроек по обновлению правил. Существует возможность автоматически получать правила с удаленного источника в сети Интернет, либо загружать заранее подготовленный файл с обновленной базой правил (см. Рисунок 63).

При получении обновления, содержащего большой объем решающих правил, обновление производится в фоновом режиме и замедляет работу **WAF Dallas Lock**. О ходе процесса свидетельствует иконка свитка в правом верхнем углу. При наведении на иконку отображается статус обновления.

Не рекомендуется в ходе процесса обновления любой из баз решающих правил осуществлять действия по конфигурации уже установленных сигнатур и их применения к защищаемым ресурсам и отдельным узлам сети.

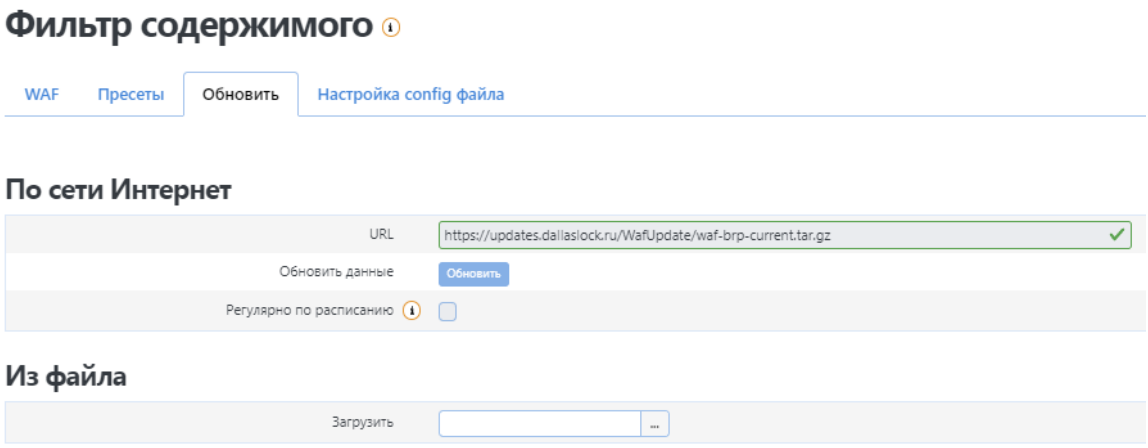


Рисунок 63. Настройка правил WAF. Фильтр содержимого. Обновить

Вкладка *Настройка config-файла* необходима для ручного описания файла конфигурации правил для **WAF** (см. Рисунок 64).

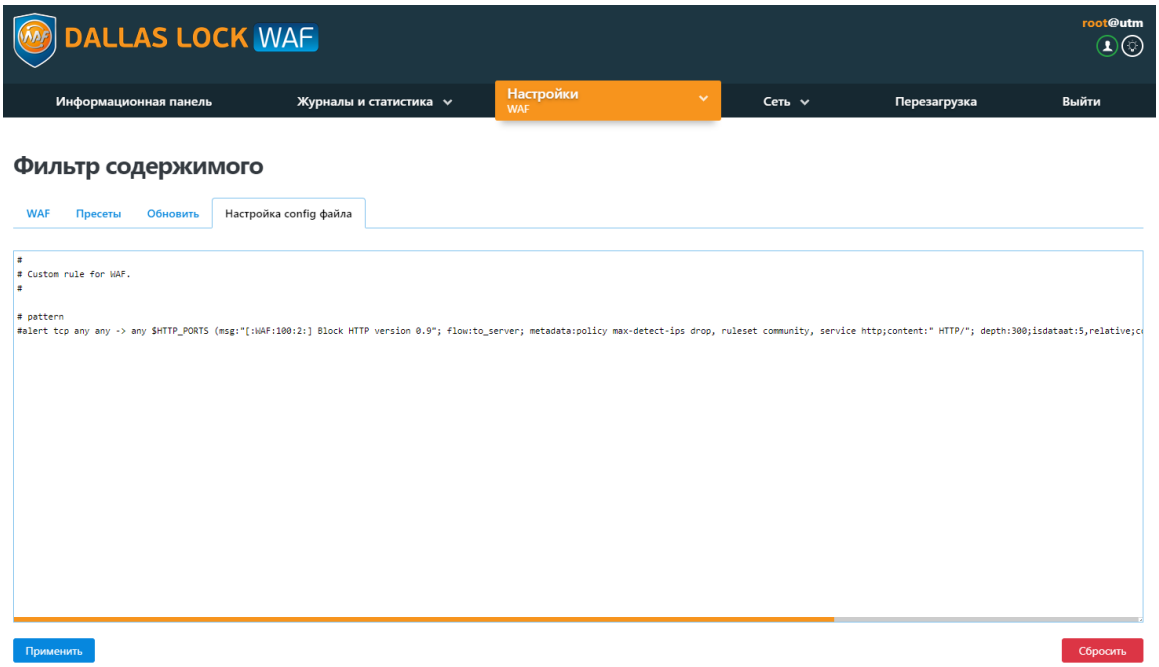


Рисунок 64. Настройка правил WAF. Фильтр содержимого. Настройка config-файла

5.1.5 Настройка инспекции защищаемого узла.

Ниже приведен общий алгоритм загрузки клиентского сертификата для инспектируемого узла.

- Открыть веб-интерфейс управления **WAF Dallas Lock**. В разделе **Настройки** выбираем пункт **WAF > Инспекция WAF > Клиенты**. Активируем опцию *Включить аутентификацию по CA*. После чего загружаем CA из файла или по URL (список отзывов сертификатов не является обязательной опцией). Нажимаем кнопку ***Применить.***
- Далее на панели ниже нажимаем кнопку **Добавить**, затем кнопку «…» и загрузить клиентский сертификат. Нажимаем кнопку **Применить.**
- Переходим к списку *Защищаемые ресурсы*. На панели загрузки новых сертификатов нажимаем кнопку выбора файла и загружаем сертификат. В новом окне нажать кнопку **Добавить**.
- В новом окне в пункте *Защищаемый сервер* выбираем наш инспектируемый узел, если он не был выбран автоматически.
- Если все было сделано правильно, то в списке защищаемых ресурсов появится инспектируемый узел. Так же он будет присутствовать во вкладке *Защищаемые серверы*.

5.2 Настройки UTM

Для перехода к разделу настроек UTM необходимо в меню **Настройки** выбрать *UTM* (см. Рисунок 65). Произойдет открытие списка меню третьего уровня.

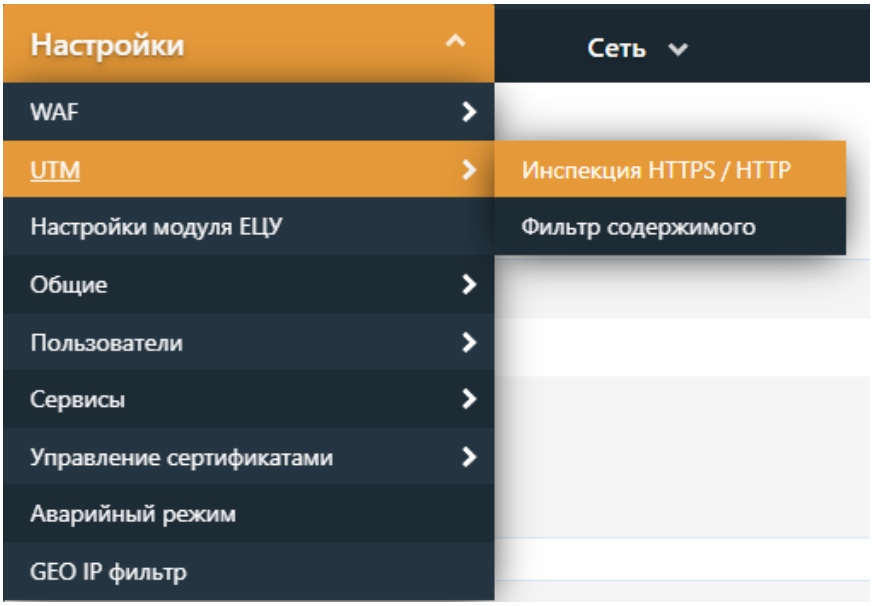


Рисунок 65. Настройка правил UTM

Данный раздел содержит следующие страницы:

- Инспекция HTTPS/HTTP;
- Фильтр содержимого.

5.2.1 Инспекция HTTPS/HTTP

Для перехвата транзитного трафика пользователей, передаваемого по протоколу http, необходимо включать чекбокс в разделе *Инспекция HTTPS/HTTP* (см. Рисунок 66).

На этой странице можно загрузить пару сертификат-ключ, используемые для перехвата и дешифрования транзитного трафика пользователей, передаваемых по протоколу SSL (HTTPS) для веб-серверов, расположенных за **WAF Dallas Lock** (более подробно в разделе 5.7.1 Серверные сертификаты). Для этого необходимо в поле *Пара сертификат-ключ* загрузить заранее подготовленный корпоративный SSL-сертификат с расширением (*.pem, *.crt, *.cert). При добавлении имя сертификата меняется на системное CA UTM WAF DL.

*Список разрешенных имен серверов***.** Данная функция позволяет обходить инспекцию HTTPS/HTTP для доверенных серверов.

Расшифровка SSL-трафика не будет работать, если не указать SSL-сертификат и приватный SSL-ключ.
На официальном сайте https://www.openssl.org можно найти документацию по сертификатам, ключам и сертификатам прокси.

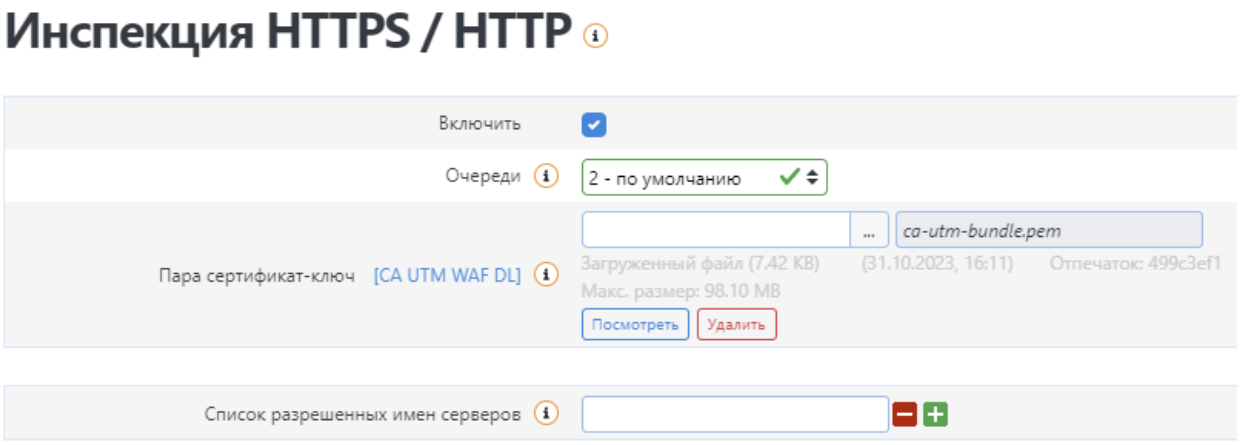


Рисунок 66. Добавление HTTPS/HTTP-сертификата

5.2.2 Фильтр содержимого

Страница *Фильтр содержимого* показывает состояние фильтра содержимого UTM и позволяет настроить уведомления о срабатывании сигнатур СОВ. Страница содержит следующие вкладки:

- опции;
- несигнатурные угрозы;
- СОВ (средство обнаружения вторжений);
- МЭ (межсетевой экран);
- пресеты;
- обновить;
- настройка config-файла.

На вкладке *Опции* (см. Рисунок 67) приведена информация о состоянии СОВ и МЭ, о количестве активных правил, общем количестве настроенных правил, количестве правил из Базы решающих правил. При нажатии кнопки **Проверить** происходит проверка введенных правил МЭ.

Также на данной вкладке можно произвести настройки уведомления о срабатывании сигнатур СОВ. В соответствующих полях указываются такие параметры, как количество срабатываний сигнатур СОВ и период (в секундах) за который это происходит.

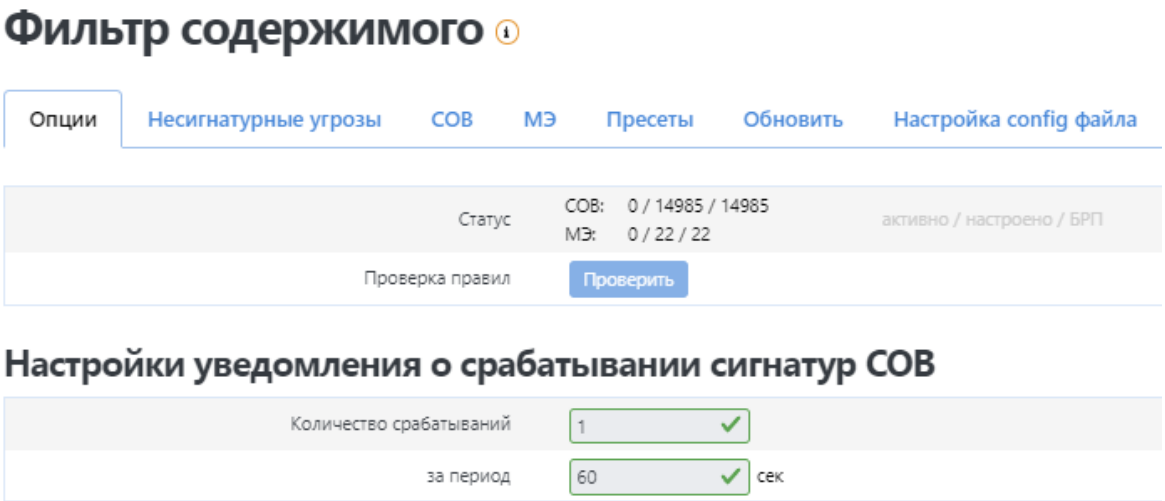


Рисунок 67. Опции

Вкладка *Несигнатурные угрозы* состоит из следующих подвкладок:

- фрагментация;
- сканирование портов;
- защита от flood-атак;
- эвристика.

На вкладке **Фрагментация** (см. Рисунок 68) настраивается фрагментация и действия при ее нарушении. Доступны следующие параметры:

- *Таймаут* — максимальное время, в течение которого будет собираться пакет.
- *Минимальный TTL* (период времени существования набора данных / пакета). Фрагменты с меньшим TTL не будут использоваться для сборки пакетов.
- *Перекрытие* — максимальный размер общих частей между фрагментами.
- *Размер* — минимальный размер фрагмента для использования при сборке пакета.

Система реагирует на следующие события:

- Несовместимые опции фрагментации.
- Атака TearDrop.
- Короткие фрагменты (возможность DOS).
- Фрагмент продолжается за размер пакета.
- Фрагмент нулевого размера.
- Фрагмент негативного размера.
- Невозможно большой фрагмент.
- Перекрытие фрагментов.
- Атака на BSD с переполнением буфера.
- Атака на BSD с лишними фрагментами.
- TTL фрагмента ниже установленного.
- Перекрытие фрагментов выше установленного.
- Фрагменты меньше установленного минимума.

Далее необходимо установить желаемые действия при нарушениях фрагментации. Возможен выбор следующих действий:

- не применять (skip);
- оповестить (alert);
- сбросить пакет (drop);
- сбросить пакет без оповещения (sdrop);
- игнорировать (pass).

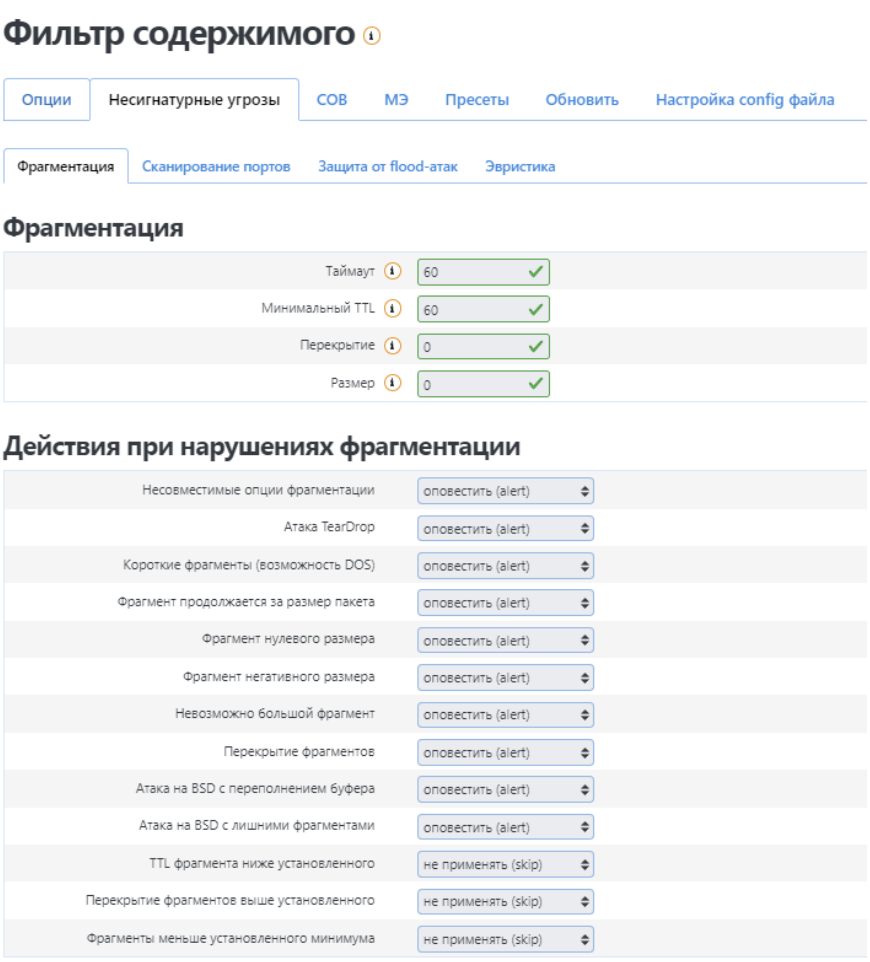


Рисунок 68. Несигнатурные угрозы – Фрагментация

На вкладке *Сканирование портов* (см. Рисунок 69) настраиваются действия при сканировании портов.

Можно включить или выключить обнаружение аномалий. Система позволяет обнаружить следующие события:

- TCP Portscan;
- TCP Decoy Portscan;
- TCP Portsweep;
- TCP Distributed Portscan;
- TCP Filtered Portscan;
- TCP Filtered Decoy Portscan;
- TCP Filtered Portsweep;
- TCP Filtered Distributed Portscan;
- IP Protocol Scan;
- IP Decoy Protocol Scan;
- IP Protocol Sweep;
- IP Distributed Protocol Scan;
- IP Filtered Protocol Scan;
- IP Filtered Decoy Protocol Scan;
- IP Filtered Protocol Sweep;
- IP Filtered Distributed Protocol Scan;
- UDP Portscan;
- UDP Decoy Portscan;
- UDP Portsweep;
- UDP Distributed Portscan;
- UDP Filtered Portscan;

- UDP Filtered Decoy Portscan;
- UDP Filtered Portsweep;
- UDP Filtered Distributed Portscan;
- ICMP Sweep;
- ICMP Filtered Sweep;
- Open Port.

Далее необходимо установить желаемые действия при сканировании портов. Возможен выбор следующих действий:

- не применять (skip);
- оповестить (alert);
- сбросить пакет (drop);
- сбросить пакет без оповещения (sdrop);
- игнорировать (pass).

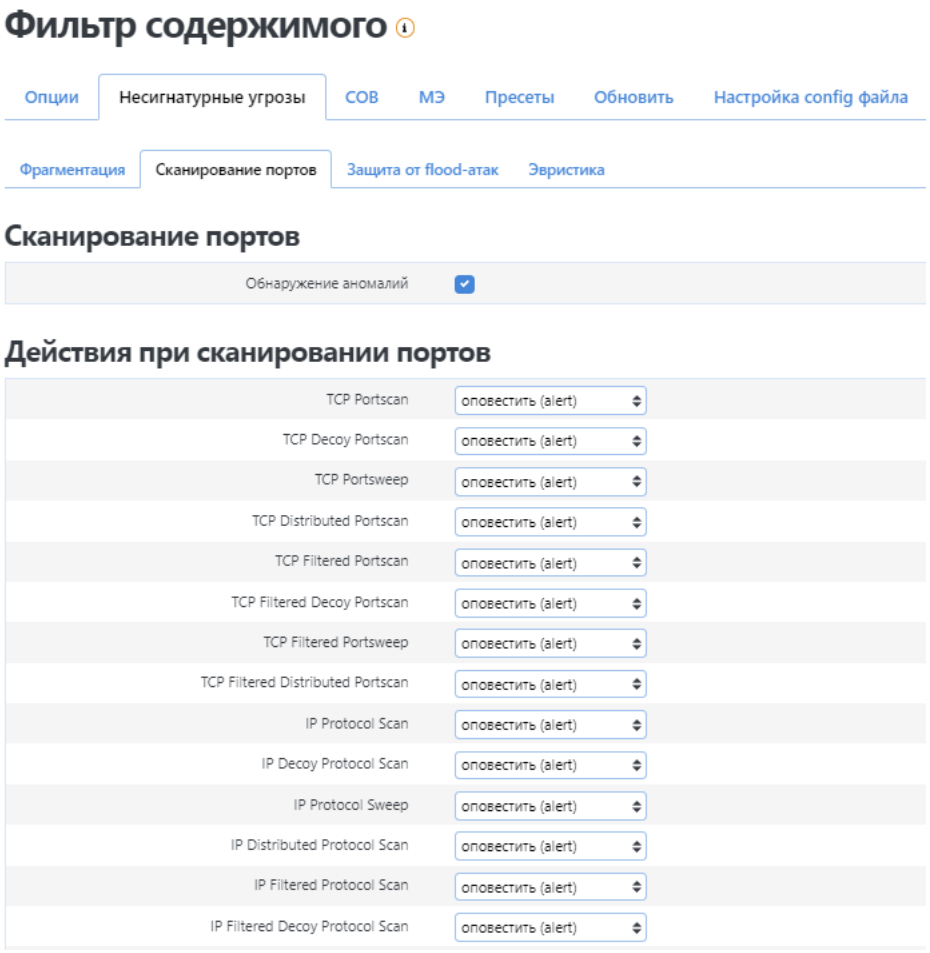


Рисунок 69. Несигнатурные угрозы – Сканирование портов

Для корректного функционирования выбранных действий при сканировании портов необходимо в блоке *Настройки переменных фильтра содержимого* выставить *Уровень эвристического анализа* в значение *Высокий* (см. Рисунок 70). Для настройки *Уровня эвристического анализа* необходимо перейти в раздел **Настройки > Общие > Фильтр содержимого.**

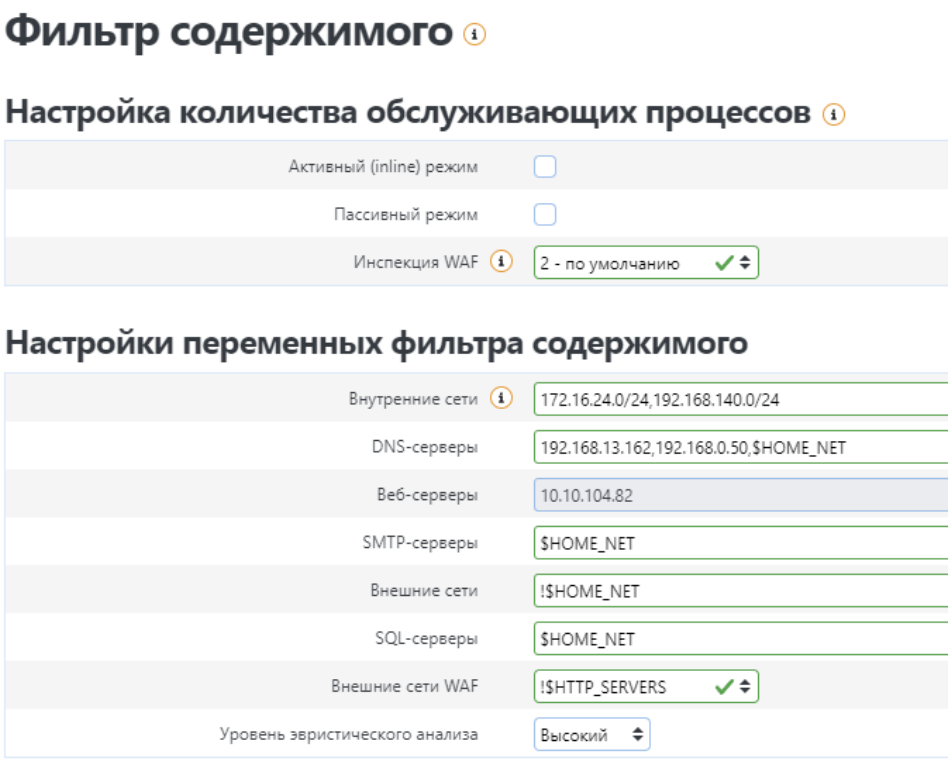


Рисунок 70. Уровень эвристического анализа

На вкладке *Защита от flood-атак* (см. Рисунок 71) настраивается защита от атак типа «отказ в обслуживании». *Защита от flood-атак* рассматривает основные способы flood-атак, нацеленные на отказ в обслуживании, позволяя отследить ненормальные действия и блокировать их. Для этого необходимо включить защиту нажав чекбокс *Включить защиту от flood-атак* и указать параметры:

- Предел пакетов.
- Пиковый предел.

Значения в полях можно задать в пределах 1-1000000.

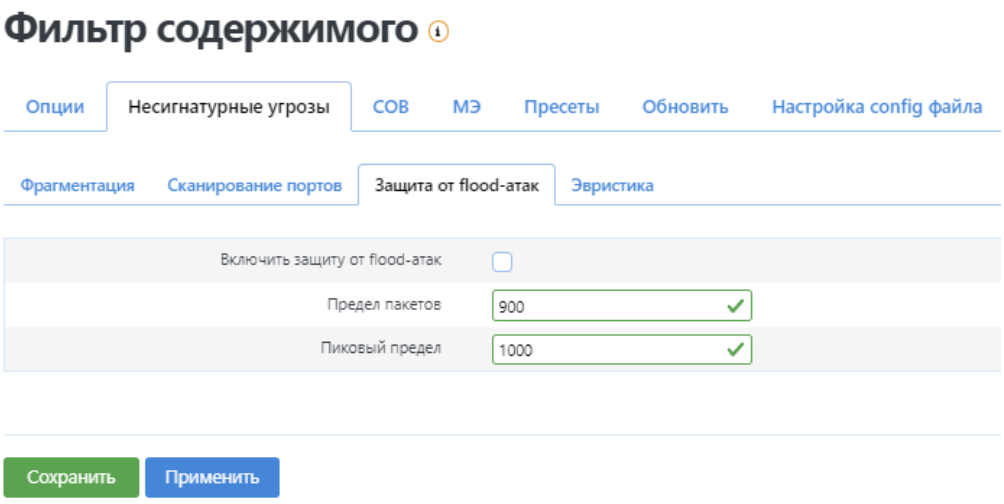


Рисунок 71. Несигнатурные угрозы. Защита от flood-атак

На вкладке *Эвристика* (см. Рисунок 72) настраивается эвристика DNS-туннелей.

Дается возможность вручную включить/отключить опцию, нажав чекбокс напротив *Включить эвристику DNS-тоннелей*, а также указать уровень чувствительности срабатываний: *низкий, средний, высокий.*

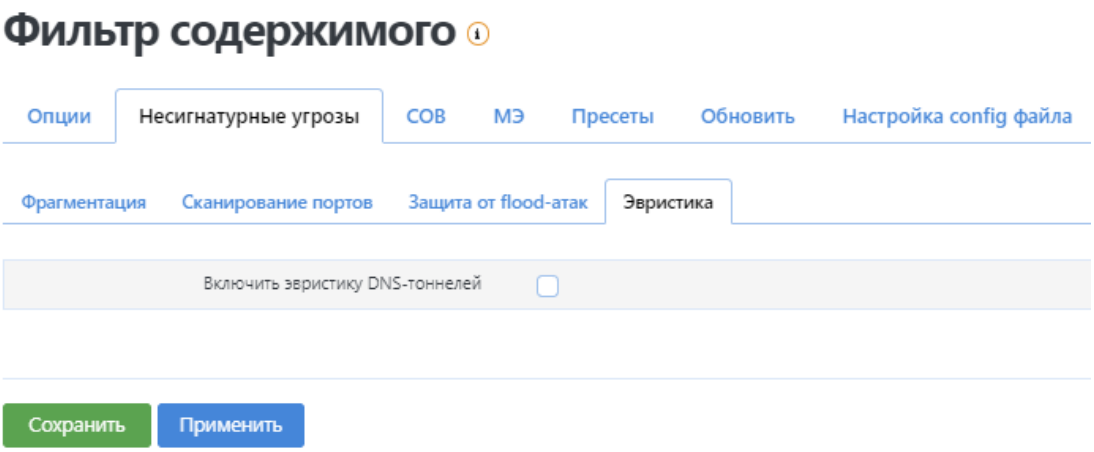


Рисунок 72. Несигнатурные угрозы. Эвристика

На вкладке *СОВ* (см. Рисунок 73) приведена информация о состоянии *Средства обнаружения вторжений*, о количестве активных правил, общем количестве настроенных правил, количестве правил из *Базы решающих правил*. Ниже представлены сигнатуры (База решающих правил), которые можно отдельно настраивать. Существует возможность изменить правила под свою инфраструктуру, задав уточняющие данные, либо включить/отключить составляющие политики для сигнатур.

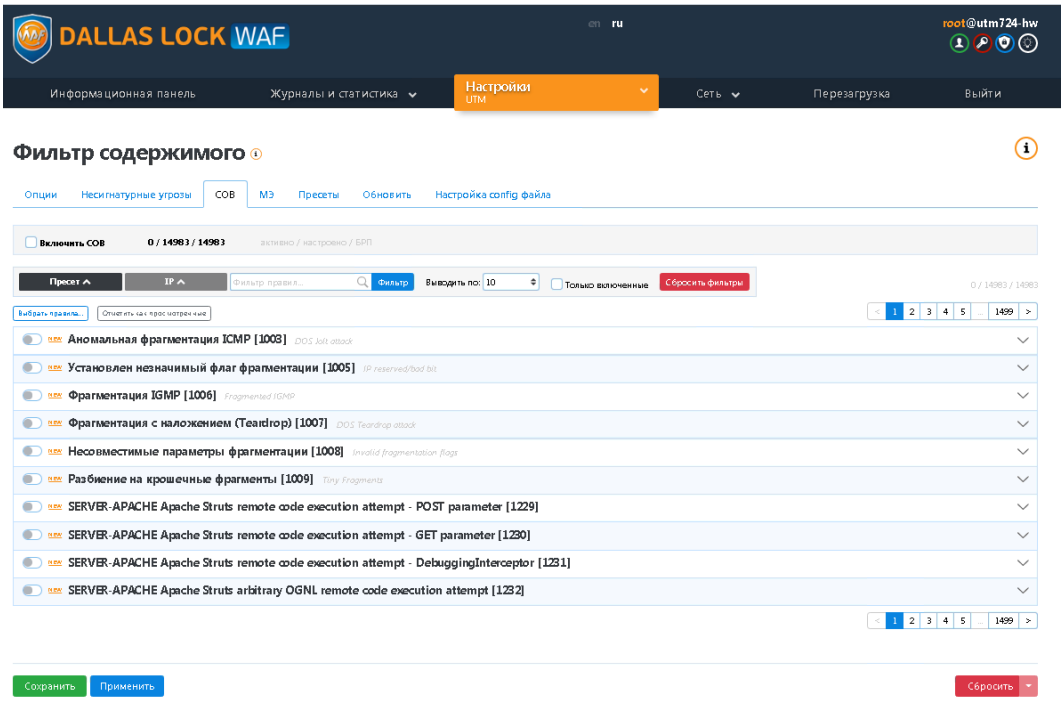


Рисунок 73. Средство обнаружения вторжений

Для изменения правила под свою инфраструктуру необходимо выбрать правило и нажать кнопку **Изменить** (см. Рисунок 74), в списке настроить параметры для сети. Для сохранения параметров нажать кнопку **Сохранить.**

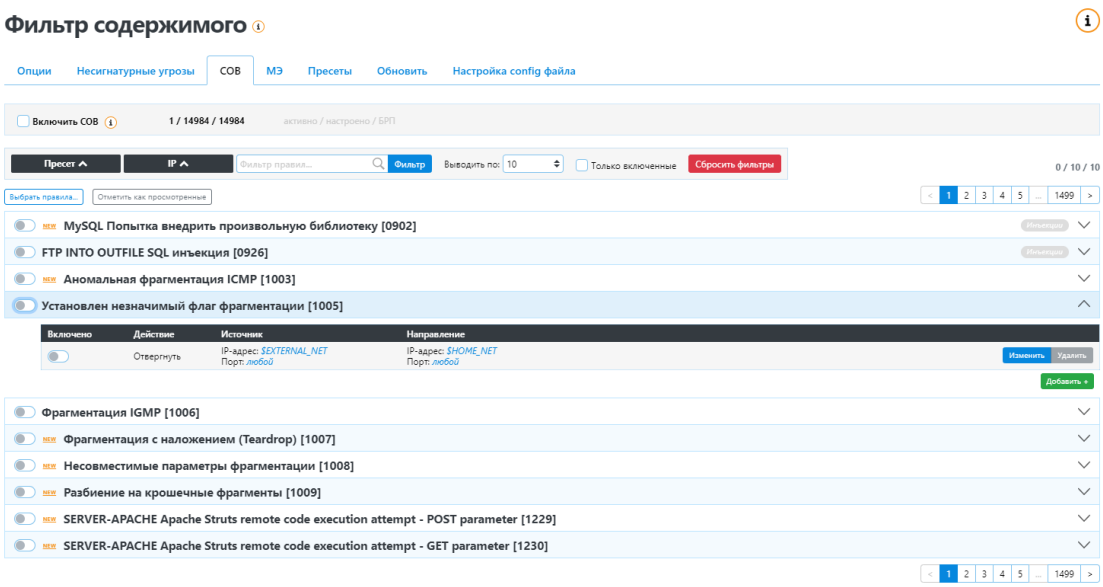


Рисунок 74. Фильтр содержимого – СОВ

Для добавления дополнительной настройки правила нажать кнопку **Добавить**, внести соответствующие изменения в параметры и нажать кнопку **Сохранить** (см. Рисунок 75). Для удаления настройки правила, нажать на кнопку **Удалить**.

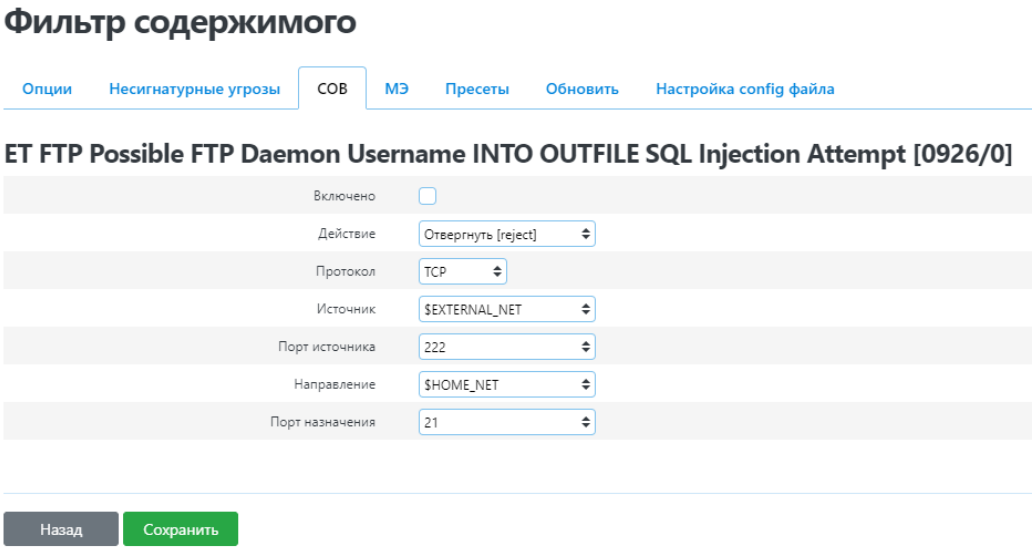


Рисунок 75. Параметры правила СОВ

На вкладке *МЭ* (см. Рисунок 76) приведена информация о состоянии Межсетевого экрана, о количестве активных правил, общем количестве настроенных правил, количестве правил из Базы решающих правил. Ниже представлены правила МЭ, которые можно настраивать отдельно. В случае необходимости существует возможность изменить правила под свою инфраструктуру, задав уточняющие данные, либо включить/отключить составляющие политики для правил МЭ.

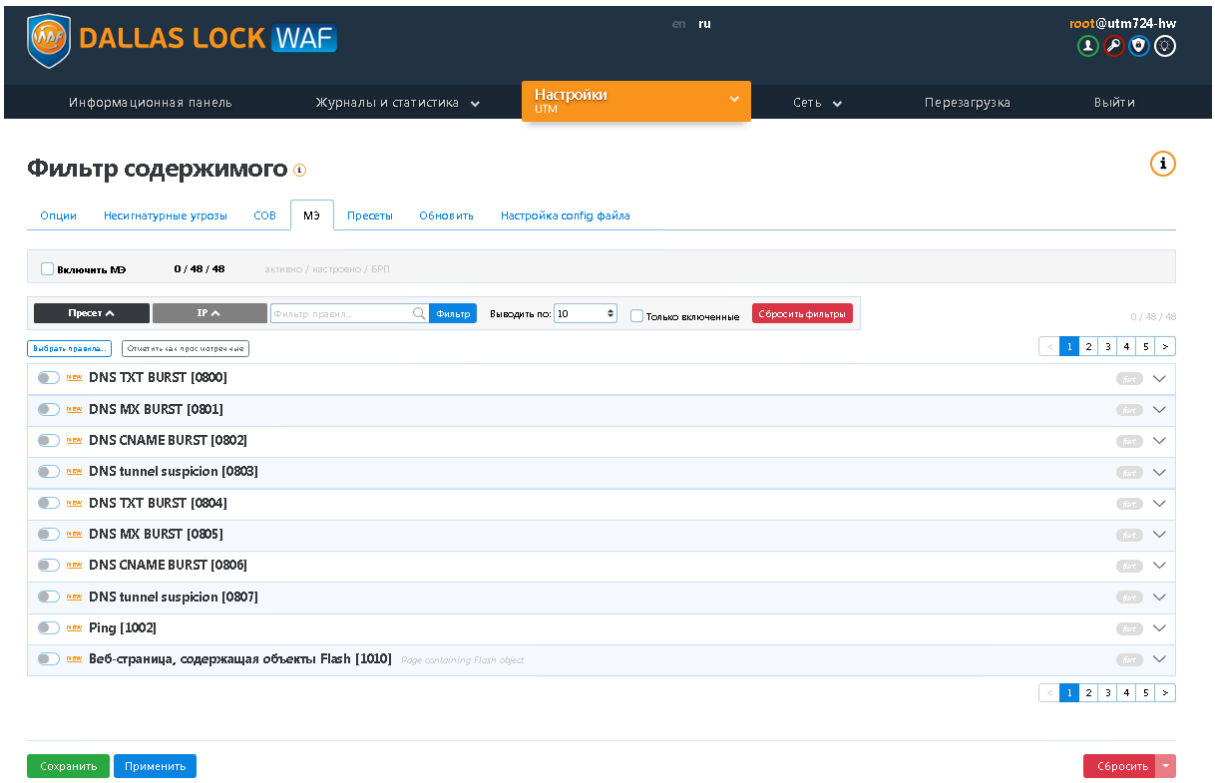


Рисунок 76. Межсетевой экран

Вкладка *Пресеты* необходима для группировки пресетов правил по видам атак. Возможно группировать не только предоставляемые пресеты, но и те, что были созданы администратором (пользовательские пресеты) (см. Рисунок 77).

Правила пресета Forbidden Data и Forbidden Methods являются сервисными пресетами. Их включение приводит к коду ответа 403 для защищаемого узла со всех адресов.

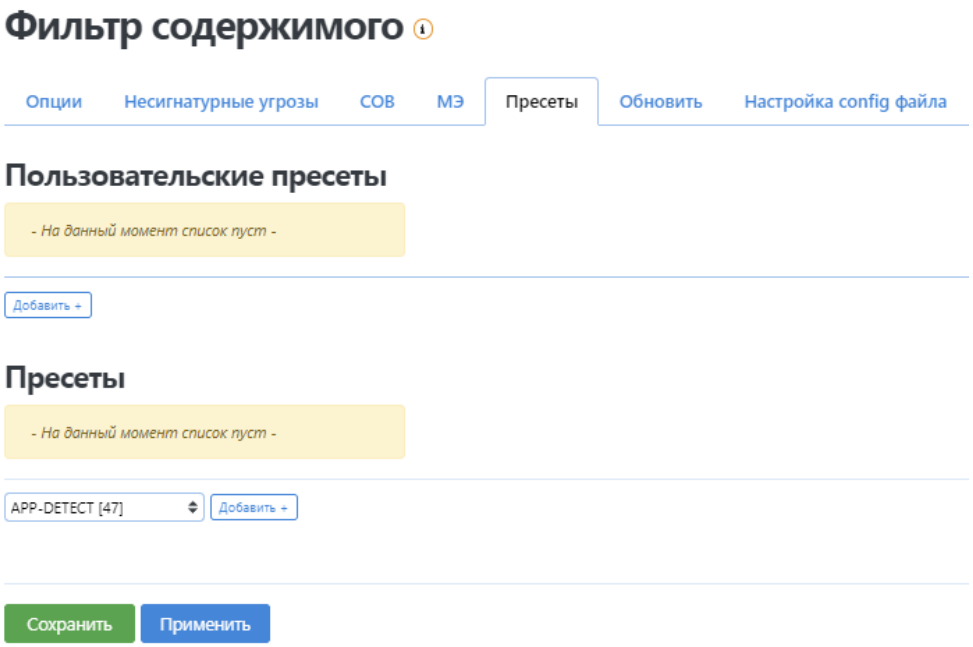


Рисунок 77. Пресеты

Вкладка *Обновить* служит для задания настроек по обновлению правил. Существует возможность

автоматически получать правила с удаленного источника в сети Интернет, либо загружать заранее подготовленный файл с обновленной базой правил (см. Рисунок 78).

При получении обновления, содержащего большой объем решающих правил, обновление производится в фоновом режиме и замедляет работу **WAF Dallas Lock**. О ходе процесса свидетельствует иконка свитка в правом верхнем углу. При наведении на иконку отображается статус обновления.
Не рекомендуется в ходе процесса обновления любой из баз решающих правил осуществлять действия по конфигурации уже установленных сигнатур и их применения к защищаемым ресурсам и отдельным узлам сети.

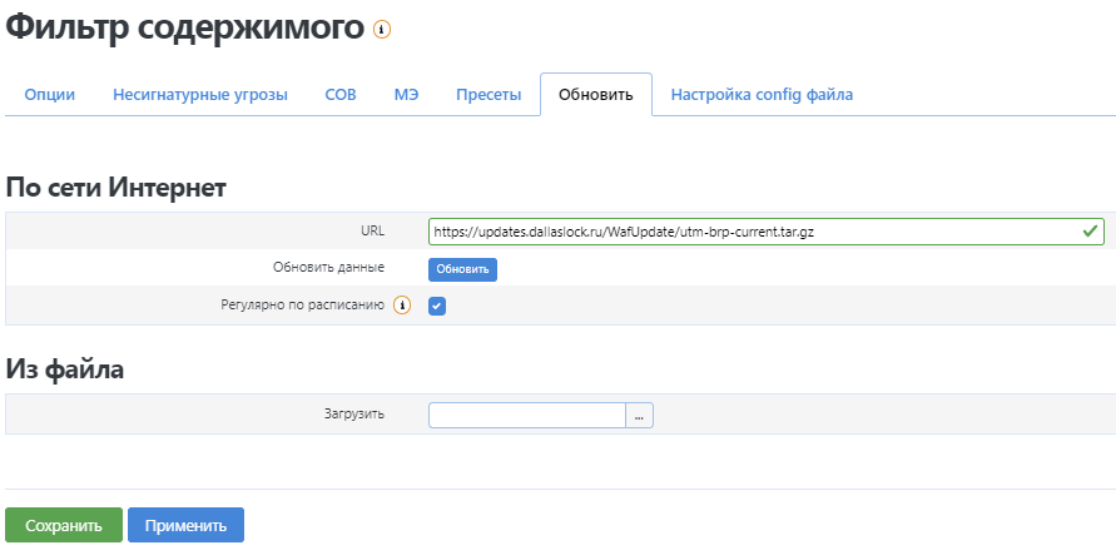


Рисунок 78. Обновить

Вкладка *Настройка config-файла* будет полезна в случае ручного описания файла конфигурации правил для UTM (см. Рисунок 79).

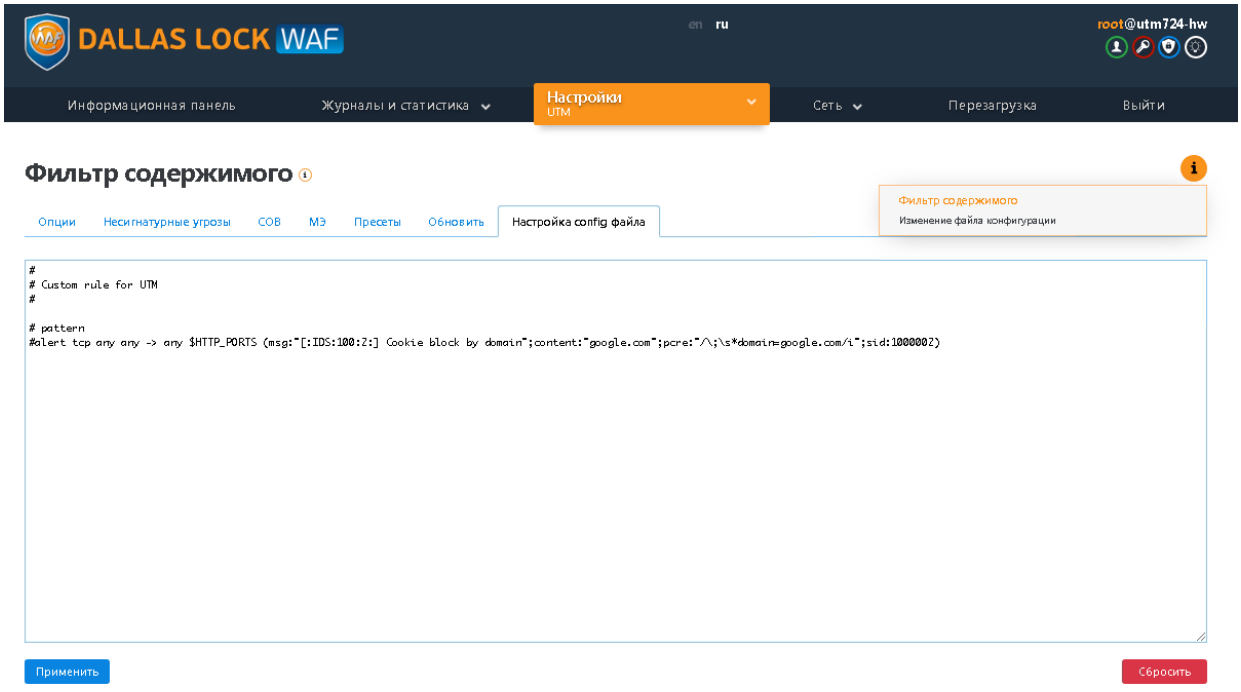


Рисунок 79. Настройка config файла

5.3 Настройки модуля ЕЦУ

5.3.1 Регистрация WAF Dallas Lock в домене безопасности ЕЦУ

Для регистрации в домене безопасности ЕЦУ в основном меню в разделе **Настройки** выберите пункт **Настройки модуля ЕЦУ** (см. Рисунок 80)

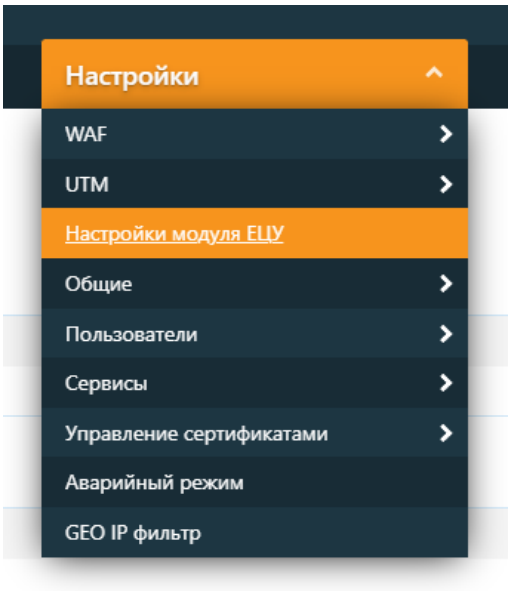


Рисунок 80. Раздел настроек, пункт Настойка модуля ЕЦУ

На странице **Настройки модуля ЕЦУ** администратору необходимо заполнить следующие поля в блоке **Настройки**:

- *Имя модуля* — сетевое имя устройства WAF Dallas Lock. Имя модуля будет отображаться в графическом интерфейсе консоли ЕЦУ.
- *Сервер ЕЦУ* — сетевой адрес сервера ЕЦУ в формате доменного имени или IP-адреса (IPv4 и IPv6). В случае, если требуется соединиться с ЕЦУ по определенному порту, можно указать порт в формате: IP-адрес:порт.
- *Ключ доступа к ДБ*. Необходимо ввести ключ доступа, задаваемый в консоли ЕЦУ.

Далее необходимо нажать кнопку **Зарегистрироваться** для регистрации устройства в домене безопасности ЕЦУ (см. Рисунок 81). Чтобы сохранить введенные настройки в форме веб-интерфейса нажмите кнопку **Сохранить**.

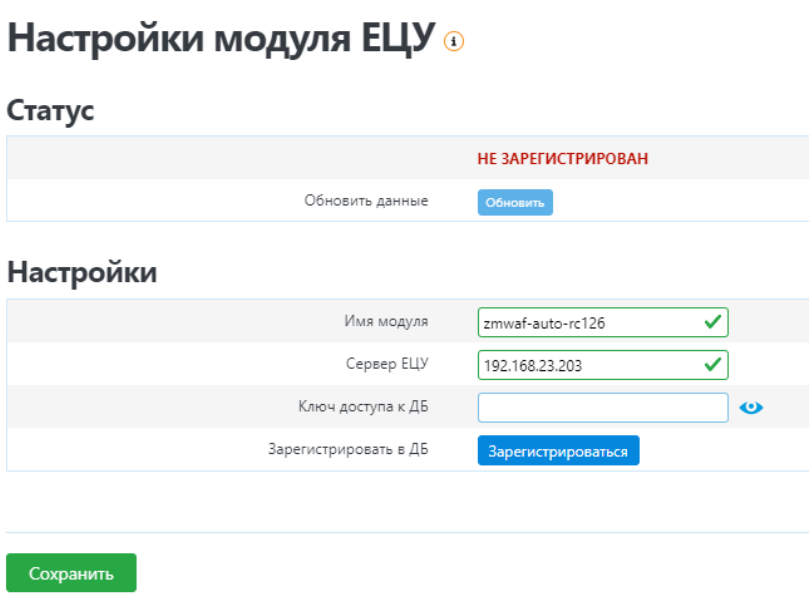


Рисунок 81. Интерфейс ввода WAF Dallas Lock в ДБ ЕЦУ

Если процесс ввода WAF Dallas Lock в ДБ прошел успешно, поля с настройками станут недоступными для редактирования (см. Рисунок 82), а в блоке **Статус** появится информация о сервере ЕЦУ Dallas Lock (см. Рисунок 83).

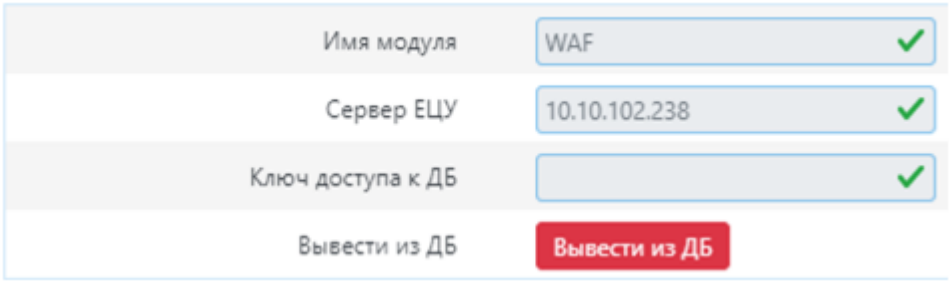


Рисунок 82. Регистрация шлюза безопасности в ДБ прошла успешно.

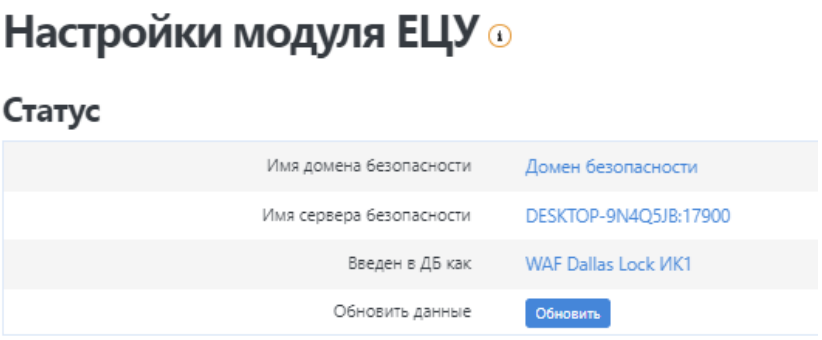


Рисунок 83. Блок Состояние при успешном вводе WAF в ДБ.

Кнопка **Обновить** позволяет актуализировать поля *Имя домена безопасности* и *Имя сервера безопасности.*

Если шлюз безопасности не введен в домен безопасности кнопка **Обновить данные** в блоке настроек *Состояние* будет не активна.

Чтобы вывести устройство из ДБ необходимо нажать кнопку **Вывести из ДБ** (см. Рисунок 82) и подтвердить действие во всплывающем окне, нажав кнопку **ОК**. После чего устройство будет выведено из домена безопасности, а администратор будет оповещен об успешном завершении операции.

Все действия (успешные и неуспешные), связанные с регистрацией и выводом шлюза безопасности из ДБ фиксируются в системном журнале. Факт потери связи с сервером ЕЦУ также будет зафиксирован в системной журнале.

5.3.2 Передача данных на ЕЦУ

После регистрации шлюза безопасности в ДБ, он отправляет на ЕЦУ свой текущий статус. Статус содержит следующую информацию:

- состояние подключения (определяется сервером ЕЦУ);
- режим работы (аварийный/нормальный режим);
- время работы (uptime);
- имя шлюза безопасности;
- IP-адрес шлюза безопасности (реализуется со стороны ЕЦУ);
- MAC-адрес шлюза безопасности (только MAC-адрес подключения);
- данные об аппаратном обеспечении (строчка устройство или «Виртуальная машина»);
- текущая версия программного обеспечения (в соответствии с данными поля *«Версия прошивки»* страницы *Состояние* графического интерфейса **WAF Dallas Lock**);
- версия базы сигнатур (номер);
- объем свободного места на диске WAF (соотношение занято/всего и, дополнительно, указанием занятого объема в процентах);
- номер лицензии (с указанием лицензированных модулей);
- код технической поддержки;
- ссылка веб-администрирования.

Отправка статуса при его изменении (кроме времени работы и объема дискового пространства) производится немедленно. Данные об объеме дискового пространства и времени работы отправляются регулярно (период синхронизации задается в настройках ЕЦУ). Также на ЕЦУ немедленно производится отправка инцидентов безопасности при их возникновении. Кроме того, через ЕЦУ отправляются сформированные блокировки (заблокированные IP-адреса и время, на которое каждый из них был заблокирован) на другие шлюзы безопасности.

5.3.3 Однокомандное управление

Шлюз безопасности **WAF Dallas Lock** принимает и выполняет следующие команды в рамках взаимодействия с ЕЦУ:

- перезагрузить шлюз безопасности;
- выключить шлюз безопасности;
- собрать журналы;
- синхронизировать;
- сбросить все временные блокировки шлюза безопасности;
- перевести шлюз безопасности в аварийный режим;
- перевести шлюз безопасности из аварийного режима в штатный;
- открыть web-администрирование.

5.3.4 Журналы

Список журналов, передаваемых шлюзом безопасности в инфраструктуру ЕЦУ:

- журнал WAF;
- журнал СОВ;
- журнал МЭ;
- журнал сетевых пакетов;
- журнал политик;
- журнал авторизации;
- системный журнал.

Реализована регулярная (период сбора журналов задается в настройках ЕЦУ) отправка содержимого перечисленных журналов с указанием важности отправляемых событий. Период сбора журналов можно задать в настройках ЕЦУ. Например, при указании важности (уровня логирования в терминологии **WAF Dallas Lock**) события «alert», на сервер ЕЦУ будут отправлены все события всех журналов, относящихся к важности (уровню логирования) «alert» и выше, то есть

на сервер ЕЦУ отправляются данные важности (уровня логирования) «alert» и «emergency».

Помимо журналов в домен безопасности ЕЦУ с WAF передаются данные о событиях безопасности (инцидентах). Обнаруженное событие безопасности передается на ЕЦУ сразу после его фиксации. В случае отсутствия связи с ЕЦУ, инциденты сохраняются и передаются при восстановлении связи.

5.3.5 Задания

Через консоль управления ЕЦУ пользователю доступно формирование следующих заданий для **WAF Dallas Lock**:

- ***Сбор журналов.*** Результатом выполнения данного задания является передача журналов шлюза безопасности.
- ***Создать резервную копию***. Результатом выполнения данного задания является создание резервной копии системы и передача ее на ЕЦУ.
- ***Восстановить резервную копию***. Результатом выполнения данного задания является отправка на шлюз безопасности и применение ранее созданной резервной копии.
- ***Сброс к заводским настройкам***. Результатом выполнения данного задания является сброс текущих конфигурационных настроек **WAF Dallas Lock**.
- ***Обновление базы решающих правил***. Инициация процедуры обновления базы решающих правил. Результатом действия является обновление базы решающих правил в случае наличия более актуальной версии.

Все действия по обработке заданий (факт выполнения задания), полученных от ЕЦУ, фиксируются системой журналирования **WAF Dallas Lock** в журнале **Системный**.

При выполнении задания с Консоли ЕЦУ на сброс к заводским настройкам, **WAF Dallas Lock** принудительно выводится из домена безопасности ЕЦУ.

5.4 Общие настройки

5.4.1 Система

На данной странице можно задать параметры устройства, такие как дата и время, имя хоста, часовой пояс, код лицензии и технической поддержки. (см. Рисунок 84)

Основные настройки:

Дата и время. Текущая дата и время.

Имя Хоста. Позволяет задать имя хоста.

Часовой пояс. Позволяет выбрать часовой пояс.

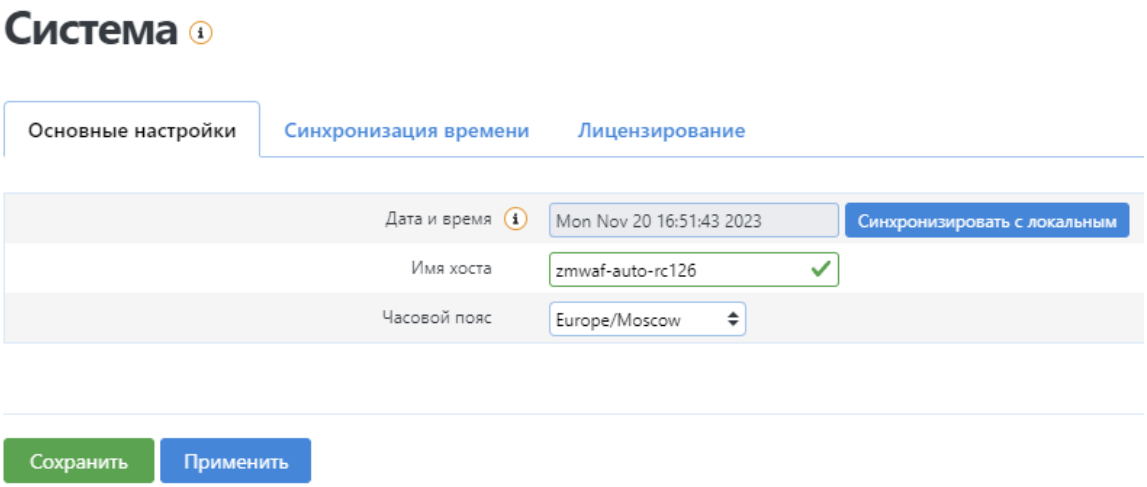


Рисунок 84. Основные настройки

Синхронизация времени.

В данном разделе (см. Рисунок 85) можно указать адрес NTP-сервера, который будет передавать временные метки для журналирования. Для этого необходимо выполнить следующие действия:

1. В строке *Синхронизация времени* выберите *NTP*.
2. Поставьте чекбокс напротив *Включить NTP-сервер*.
3. В строке *Список NTP-серверов*, задайте IP-адрес или имя сервера времени.

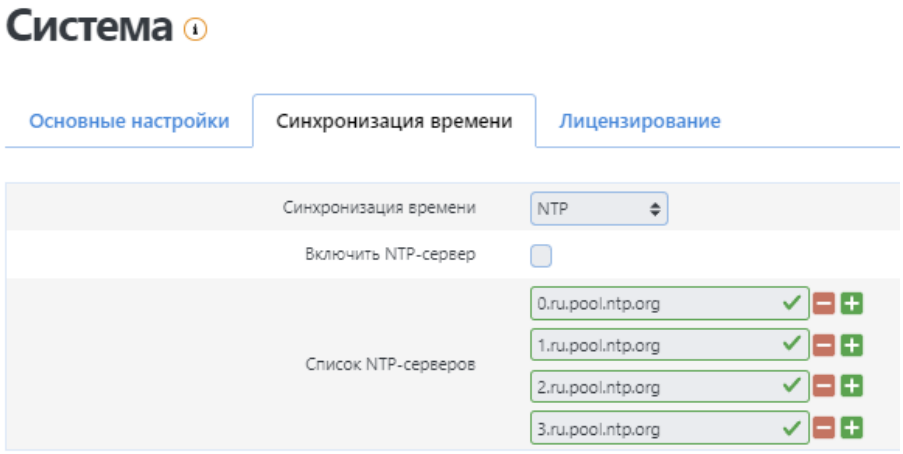


Рисунок 85. Синхронизация времени

В случае, если **WAF Dallas Lock** введен в домен ЕЦУ Dallas Lock, в списке появится возможность выбрать ЕЦУ для синхронизации времени.

Лицензирование

Данная вкладка (см. Рисунок 86) позволяет пользователю получить информацию о лицензировании продукта, подключенных модулях защиты, даты окончания срока лицензии. В строке *Номер лицензии*, можно задать номер лицензии. В строке *Код поддержки*, можно задать код технической поддержки продукта.

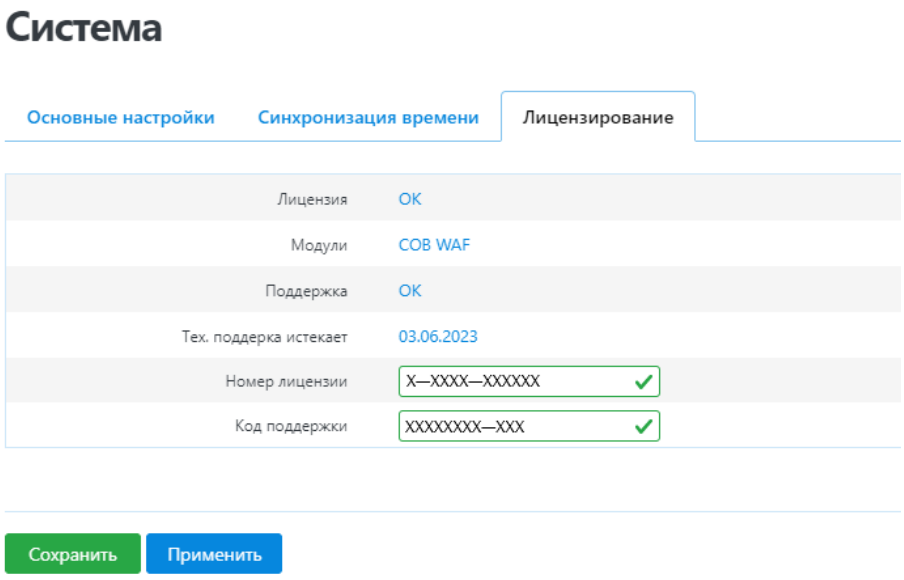


Рисунок 86. Лицензирование

5.4.2 Настройки интерфейса управления WAF Dallas Lock

На данной странице производятся настройки управления через веб-интерфейс или подключение к

WAF Dallas Lock по протоколу SSH.

5.4.2.1 Базовые настройки

На вкладке *Базовые* можно:

- задать или сгенерировать пароль администратора **WAF Dallas Lock** (см. Рисунок 87);
- включить/выключить доступ по проколу SSH (см. Рисунок 88). По умолчанию доступ по протоколу SSH выключен;
- сконфигурировать доступ к сервису SSH (см. Рисунок 89), указав в настройках:
  - *Интерфейс.* Можно указать, через какой сетевой интерфейс будет возможно подключение к **WAF Dallas Lock** по проколу SSH. По умолчанию «lan».
  - *Порт.* Указывается порт сервиса. По умолчанию «22».
  - *С помощью пароля.* При включении данной функции разрешается SSH-аутентификация по логину и паролю аудитора **WAF Dallas Lock**.
  - *Root входит по паролю.* При включении данной функции разрешается SSH-аутентификация по логину и паролю администратора **WAF Dallas Lock**.
  - *Таймаут неактивной сессии.* Можно указать ограничение неактивной сессии в минутах, по истечении которого сессия будет «разорвана».

В поле *SSH-ключи* можно добавить ранее сгенерированные SSH-ключи (один ключ на строку) для SSH-аутентификации.
Для каждого интерфейса задаются отдельные настройки. Для того чтобы добавить интерфейс необходимо нажать кнопку **Добавить секцию**, выбрать интерфейс и указать настройки.

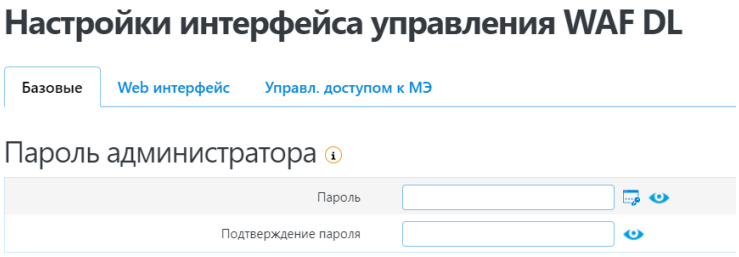


Рисунок 87. Пароль администратора

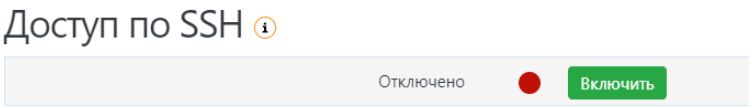


Рисунок 88. Доступ по SSH

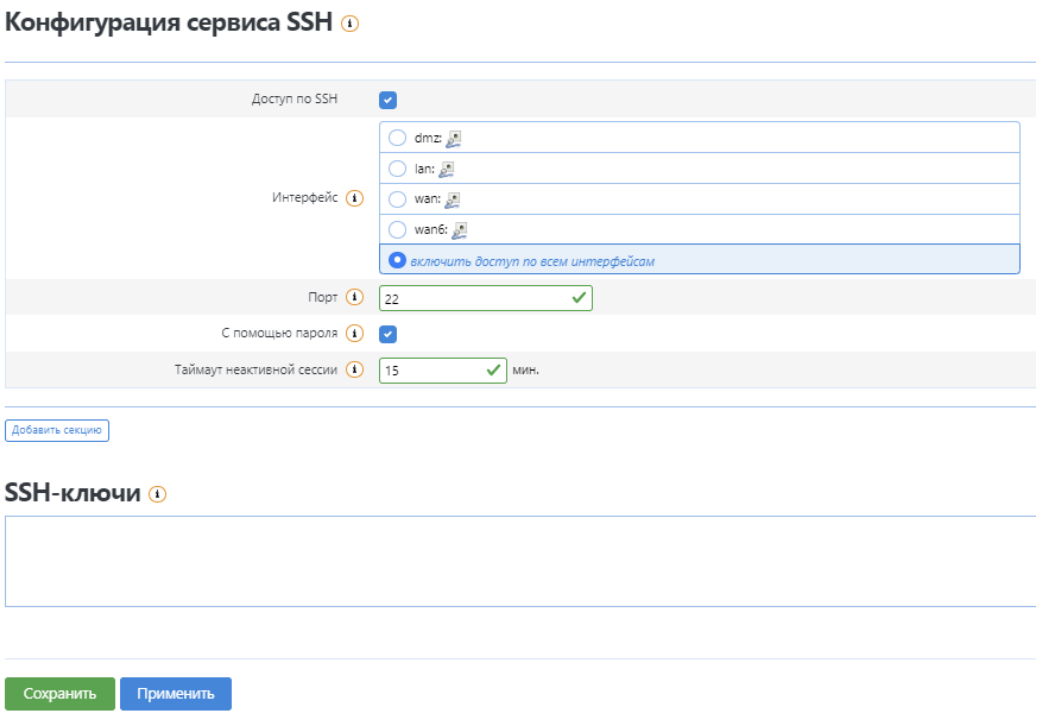


Рисунок 89. Конфигурация сервиса SSH

При невозможности управления **WAF Dallas Lock** в аварийном режиме через веб-интерфейс, или по желанию пользователя, может быть выполнено подключение к **WAF Dallas Lock** по протоколу SSH. Для получения доступа по протоколу SSH пользователь должен обладать правами администратора, то есть при подключении он должен ввести логин и пароль администратора **WAF Dallas Lock.**

Доступна одновременная авторизация через консоль управления по протоколу SSH и через веб-интерфейс непосредственно на сервере. Одновременное управление доступно только в аварийном режиме (см. 5.7 Настройка аварийного режима).

Так же есть возможность использовать эмулятор терминала Linux ISH Shell (консольная оболочка администрирования). Настройки возможно производить только в аварийном режиме.

Сценарии:

- При аварийном режиме пользователь производит авторизацию с клиентского ПК на **WAF Dallas Lock** через веб-интерфейс или через SSH (подключение через SSH доступно только при включении аварийного режима работы).
- Также администратор может одновременно открыть сессию на самом сервере **WAF Dallas Lock** и производить настройки в ISH Shell.
- Есть ограничения по работе с ISH Shell, в ней нельзя вносить настройки в обычном режиме. Работа только по указанным командам.

Ряд команд (команды с ограничениями представлены в таблице 3) можно выполнить, только создав учетную запись Администратора сервера (subadmin).

При выполнении команд *create-subadmin* и *remove-subadmin* интерфейс управления позволяет выполнить функцию создания и удаления учетной записи пользователя для администрирования сервера N раз, но создается и удаляется только одна учетная запись.

При подключении через консольную оболочку ISH Shell, пользователю доступны следующие команды (представлены в таблице 3). Список служб и их описание представлены в таблице 4 раздела 5.4.6 Управление службами.

Таблица 3. Список команд

Команда	Описание	Параметры
help	Выводит полный список команд,	отсутствуют

	доступных на текущем уровне (напротив каждой команды следует пояснение)	
list	Список команд доступных на текущем уровне	отсутствуют
return	Переход на верхний уровень в иерархии оболочки (на самом верхнем уровне не происходит никакого действия)	отсутствуют
Команды уровня waf-settings (без ограничений)		
backup-config	Команда сохранения резервного архива текущей конфигурации (параметр)	*path* — строковая величина: указывается путь и имя файла для сохранения в него архива конфигурации *Пример:* *backup-config"/путь/имя файла"*
backup-logs	Команда сохранения резервного архива журналов на локальном жестком диске	отсутствуют
emerge-off	Команда выключения аварийного режима	отсутствуют
emerge-on	Команда включения аварийного режима	отсутствуют
exit	Выход с любого уровня оболочки, с необходимостью авторизации после выхода	отсутствуют
factory-reset	Команда сброса системы к заводским установкам	отсутствуют
load-rj	Загрузка правил	*all* — булева величина в формате yes/no: загрузка всех правил; *force* — булева величина в формате yes/no: обязательность загрузки правил; *utm* — булева величина в формате yes/no: правила UTM; *utm_rev2* — булева величина в формате yes/no: правила UTM rev.2 (при сбросе на заводские настройки); *waf* — булева величина в формате yes/no: правила WAF; *waf_rev2* — булева величина в формате yes/no: правила WAF rev.22 (при сбросе на заводские настройки).
maintenance	Зарезервированная команда	отсутствуют
mgmt-ip	Добавление ip-адреса в список адресов, с которых возможно администрирование системы	ip — строковая величина: ip-адрес
reboot	Перезагрузка системы	отсутствуют
reset-logs	Удаление журналов	отсутствуют

resize-var	Оптимизация размера /var (расширение раздела для хранения журналов на весь жесткий диск)	отсутствуют
restart-service	Перезапуск сервиса	service — строковая величина: имя сервиса
shutdown	Выключение системы	отсутствуют
syslog-archive	Архивирование журналов в файл с датой в имени в директорию /var/archive/syslog	отсутствуют
Команды с ограничениями (выполнение команд только администратором сервера)		
create-subadmin	Создание учетной записи пользователя subadmin и группы subadmin для администрирования сервера	отсутствуют
get-cpuload	Вывод на экран суммарной загрузки процессора на момент вызова команды	отсутствуют
get-freediskspace	Вывод на экран количества байт свободного места на диске	отсутствуют
get-freemem	Вывод на экран количества байт свободной оперативной памяти на момент вызова команды	отсутствуют
remove-subadmin	Удаление учетной записи пользователя subadmin и группы subadmin для администрирования сервера	отсутствуют
Команды конфигурирования		
execute	Вызов команды	
preview	Просмотр параметров конфигурируемой команды	
Команды синонимы (alias)		
r — return	Переход на верхний уровень в иерархии оболочки	отсутствуют
x — exit	Команда выполняет выход с любого уровня оболочки, с необходимостью авторизации после выхода	отсутствуют

При резервном копировании конфигурации **WAF Dallas Lock** сохраненные ключи аутентификации SSH не сохраняются и требуют повторного импорта на **WAF Dallas Lock.**

5.4.2.2 Web-интерфейс

На вкладке *Web-интерфейс* настраивается доступ к интерфейсу по протоколам HTTP и HTTPS и возможность загружать и генерировать запрос на SSL-сертификат.
Основные настройки (см. Рисунок 90):

- *Входящие HTTP и Входящие HTTPS.* Задаются адреса в формате (адрес:порт) для доступа к веб-интерфейсу по протоколам HTTP и HTTPS.
- *Игнорировать приватные IP-адреса при публичном интерфейсе.* Эта функция не позволяет подделать IP-адрес источника с целью обмана системы безопасности. При

включении данной функции игнорируются запросы с локального IP-адреса, находящегося в WAN зоне (по умолчанию включена).

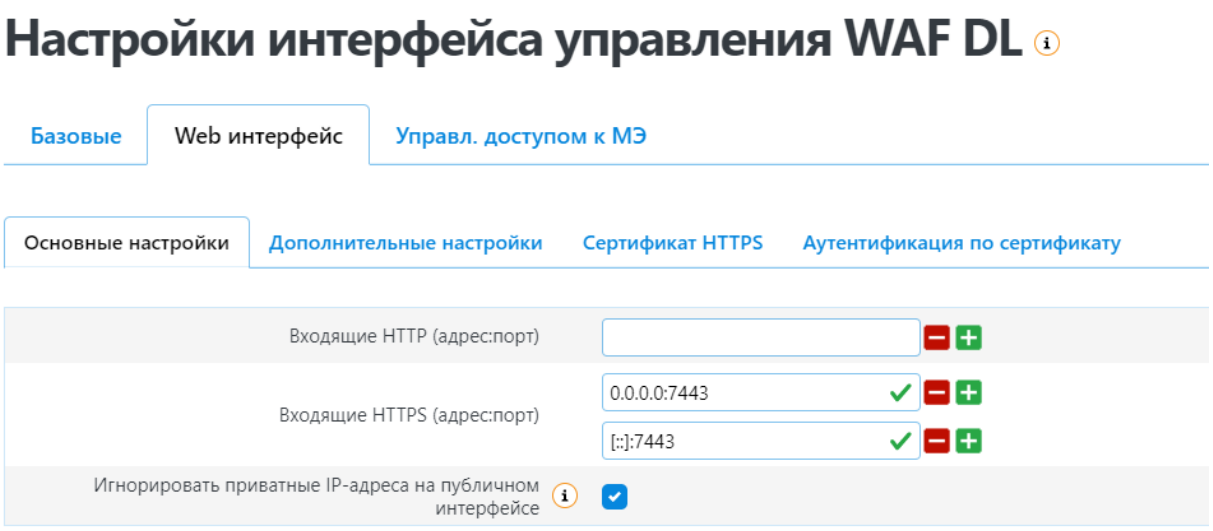


Рисунок 90. Основные настройки

*Дополнительные настройки***.** Задаются дополнительные настройки сессии администратора при авторизации к интерфейсу **WAF Dallas Lock** по протоколу HTTPS (см. Рисунок 91).

- *Время действия авторизации.* Время сессии при закрытой вкладке браузера.
- *Максимальное время ожидания загрузки.* Время, за которое запрос веб-страницы будет обработан. По истечении заданного времени, если запрос будет не обработан, страница выдаст ошибку.
- *Максимальное время ожидания сетевой активности.* Соединение разрывается, если в течение указанного количества секунд не происходило никакой сетевой активности.
- *Открыть доступ к UI.* Указание того, в течение которого времени определенный IP-адрес будет находиться в «белом» списке.
- *Повторное использование соединения.* Повторное использование соединения по протоколу HTTP.
- *TCP Keepalive.* Повторное использование соединения по протоколу TCP. Установленное значение 0 отключает данную функцию.
- *Максимальное количество соединений.* Если число превышено, дальнейшие попытки TCP-соединения ставятся в очередь до тех пор, пока количество активных соединений снова не упадет ниже этого предела.
- *Максимальное количество запросов скрипта.* Максимальное количество одновременных запросов к веб-интерфейсу. Если это число превышено, дальнейшие попытки TCP-запросов ставятся в очередь до тех пор, пока количество запросов снова не упадет ниже этого предела.

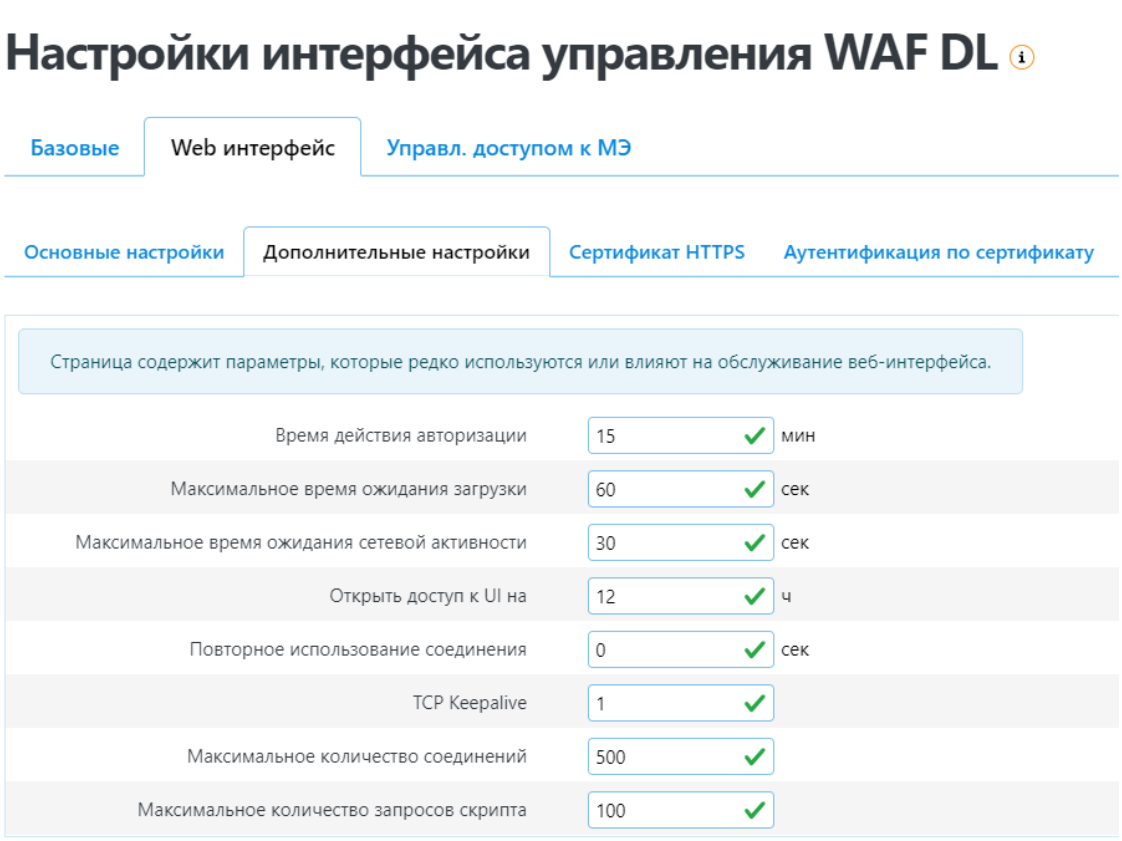


Рисунок 91. Дополнительные настройки

Сертификат HTTPS. На данной вкладке (см. Рисунок 92) администратор **WAF Dallas Lock** может сгенерировать CSR-запрос клиентского SSL-сертификата для аутентификации и идентификации безопасного HTTPS-подключения администратора к веб-интерфейсу **WAF Dallas Lock**.

Получить подписанный сертификат и запрос на подпись можно несколькими способами: воспользоваться услугой сторонних УЦ, отправив им запрос (CSR-файл) и получив в ответ готовый сертификат либо создать сертификат внутренним УЦ компании (самоподписанный сертификат).
Важно отметить, что сертификаты, подписанные аккредитованным УЦ, известны веб-браузерам. Самоподписанные сертификаты необходимо импортировать в хранилище доверенных сертификатов веб-браузера вручную. Поскольку соединения с доменами, обслуживаемыми такими сертификатами по умолчанию блокируются.

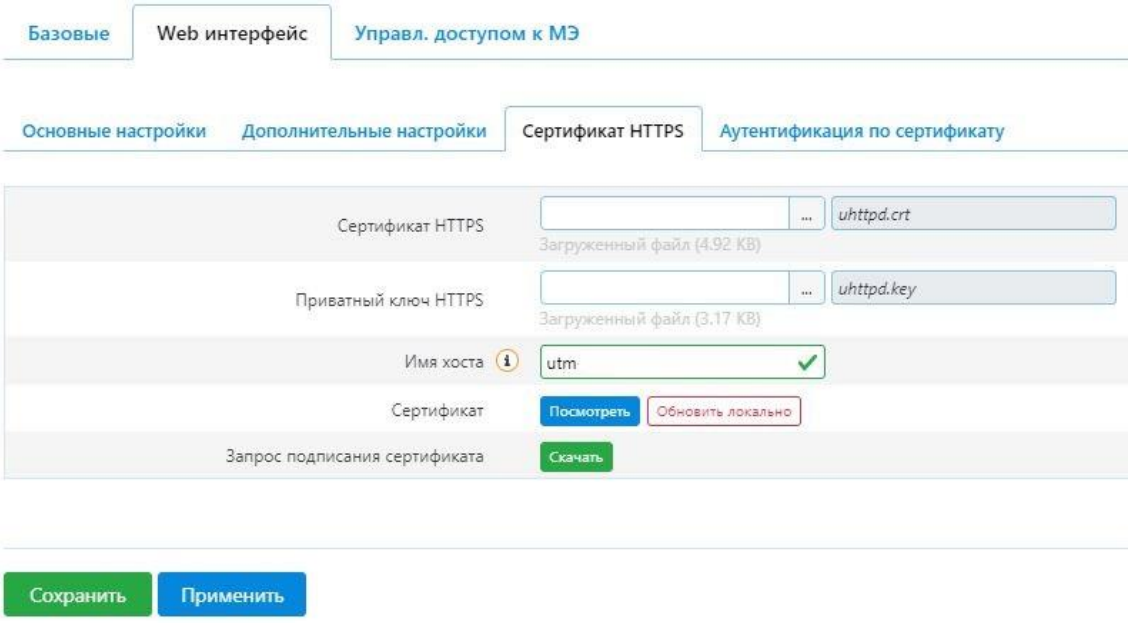


Рисунок 92. Сертификат HTTPS

Рекомендуется сохранять сертификат и ключ сертификата для возможности его последующего восстановления.

В строке *имя хоста* использование «.» в имени сервера при аутентификации по сертификату *CA Root* приводит к предупреждению, что сертификат недействителен (см. Рисунок 93). При этом полное имя сервера host.local, где local имя домена, не приводит к подобной ошибке.

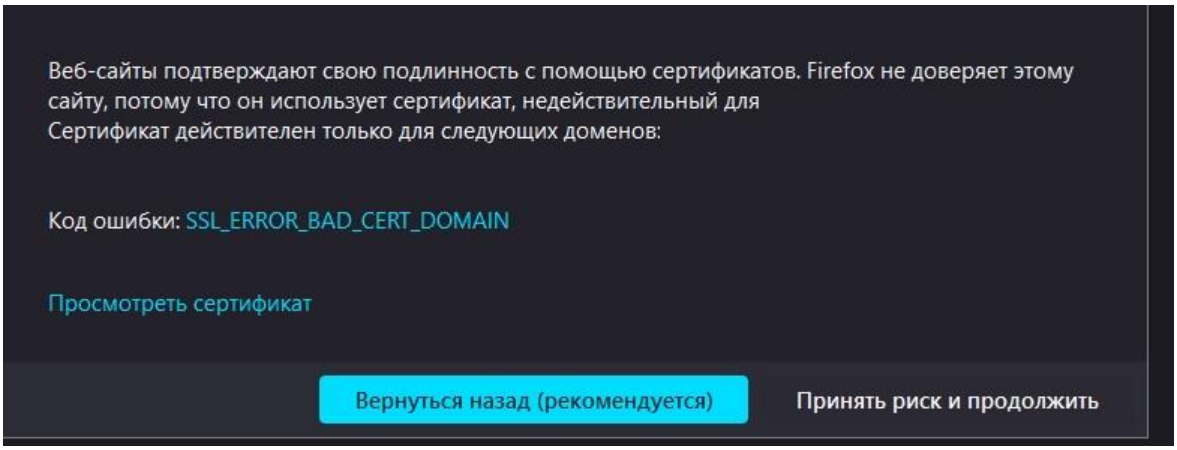


Рисунок 93. Ошибка SSL сертификата.

Аутентификация по сертификату. Дополнительной мерой усиления безопасности доступа к веб-интерфейсу управления может быть включение режима авторизации администратора с использованием SSL-сертификата. В строке *Сертификат* необходимо выбрать ранее сгенерированный на вкладке *Сертификат HTTPS*, клиентский SSL-сертификат (см. Рисунок 94).

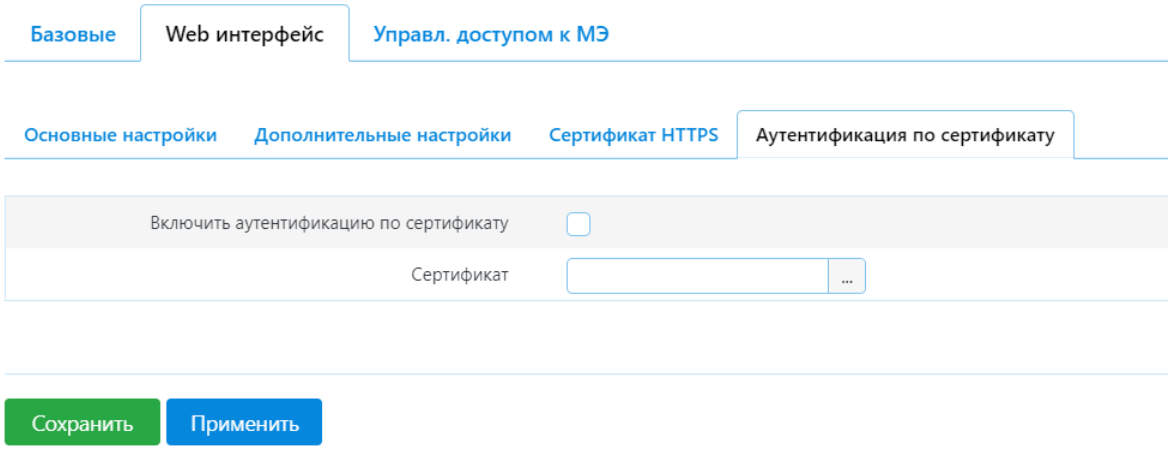


Рисунок 94. Аутентификация по сертификату

Для создания клиентского сертификата необходимо выполнить следующие шаги (на примере утилиты OpenSSL):

- Выполнить команду для создания закрытого ключа внутреннего УЦ: **openssl genrsa -out CA.key 4096**.
- Выполнить команду для создания промежуточного сертификата УЦ: **openssl req -x509 -new -key CA.key -days 1825 -out CA.crt**.
- Выполнить команду для создания клиентского закрытого ключа для инспектируемого сетевого узла: **openssl genrsa -out client.key 4096**.

- Выполнить команду для создания запроса на подпись CSR-файл, который будет включать только что сгенерированный открытый клю.ч для инспектируемого сетевого узла: **openssl req -new -key client.key -out client.csr**.
- Выполнить команду для генерации подписанного сертификата для инспектируемого сетевого узла: **openssl x509 -req -in client.csr -CA CA.crt -CAkey CA.key -CAcreateserial -out client.crt -days 365** *(*параметр x509 задает формат генерируемого сертификата*;* параметр -days указывает количество дней, в течение которых выпускаемый сертификат будет действителен).
- Возможно сторонний УЦ предоставит данные в бинарном формате PKCS # 12 (файлы *.pfx или *.p12). Если мы уже имеем такой формат ключей для каждого сетевого узла, с которого мы планируем администрировать WAF DL через веб-интерфейс, то можно переходить к следующему шагу. Если нет, то необходимо выполнить команду конвертирования закрытого ключа (файл *.key) и открытого ключа (файл *.crt/*.cer) в формат *.p12/*.pfx: **openssl pkcs12 -export -out client.p12 -inkey client.key -in client.crt**.
- Выполнить команду для сборки клиентского сертификата в котором содержится ключ и сам сертификат: **openssl pkcs12 -export -out client1.p12 -inkey client.key -in client.crt**.
- На вкладке *Аутентификация по сертификату* (см. Рисунок 94) необходимо поставить чекбокс *Включить аутентификацию по сертификату,* в строке *Сертификат* выбрать ранее созданный CA сертификат.
- Далее необходимо импортировать клиентский сертификат в хранилище ОС «Доверенные корневые центры сертификации» с которого будет выполняться авторизация в веб-интерфейс **WAF Dallas Lock**.

В процессе импорта сертификата есть опция усиленной защиты закрытого ключа. Не рекомендуется активировать эту опцию если на данном АРМе установлено СЗИ НСД DL 8.0. В противном случае могут возникнуть проблемы в процессе аутентификации **WAF Dallas Lock** и потребуется вносить дополнительные настройки в реестр ОС.

5.4.2.3 Управление доступом к межсетевому экрану

На вкладке **Управление доступом к МЭ** (см. Рисунок 95) можно разрешить доступ к веб-интерфейсу только из локальной сети (режим LAN активен по умолчанию). При выборе режима *Выключено* доступ к МЭ будет неограничен.

- *Дополнительный доступ*. В списке будут отображаться дополнительные сети/узлы, которым открыт доступ к управлению МЭ WAF DL.
- *Новое правило доступа*. Данная функция позволяет добавить IP-адрес клиента для доступа к веб-интерфейсу из внешней сети. Для этого введите внешний IP-адрес/Сеть и нажмите кнопку **Добавить** (см. Рисунок 95. Управление доступом)

При нажатии кнопки **Сохранить** происходит сохранение введенных настроек в форме веб-интерфейса. При нажатии кнопки **Применить** происходит запись введенных настроек в соответствующие config-файлы.

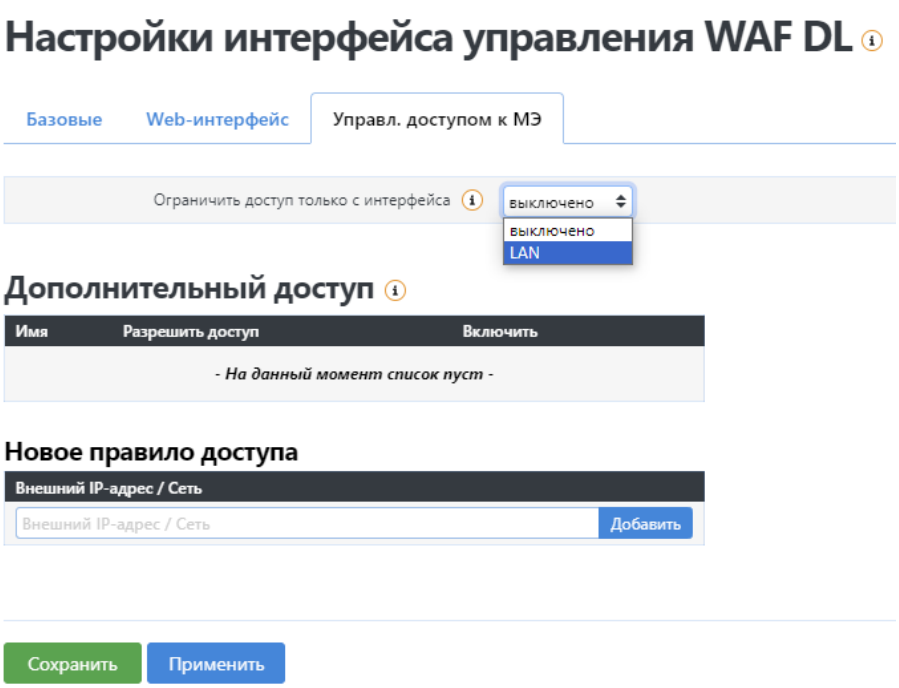


Рисунок 95. Управление доступом

После того как внешний IP-адрес добавлен, откроется окно *Межсетевой экран — Параметры управления доступом* (см. Рисунок 96), где можно задать производное имя сети, а также включить/отключить правило.

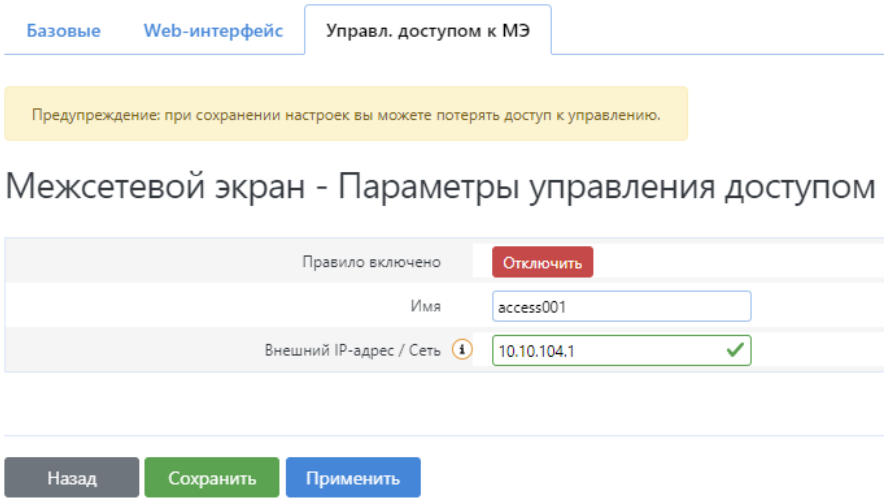


Рисунок 96. Параметры управления доступом

Обратите внимание, что при сохранении настроек вы можете потерять доступ к управлению.

5.4.3 Параметры аудитора

Страница *Параметры аудитора* доступна из основного меню (см. Рисунок 97). Содержит настройки аудита и обработки инцидентов безопасности. На странице доступны следующие вкладки:

- Настройки журнала;
- Архивирование журналов;
- Обработка инцидентов.

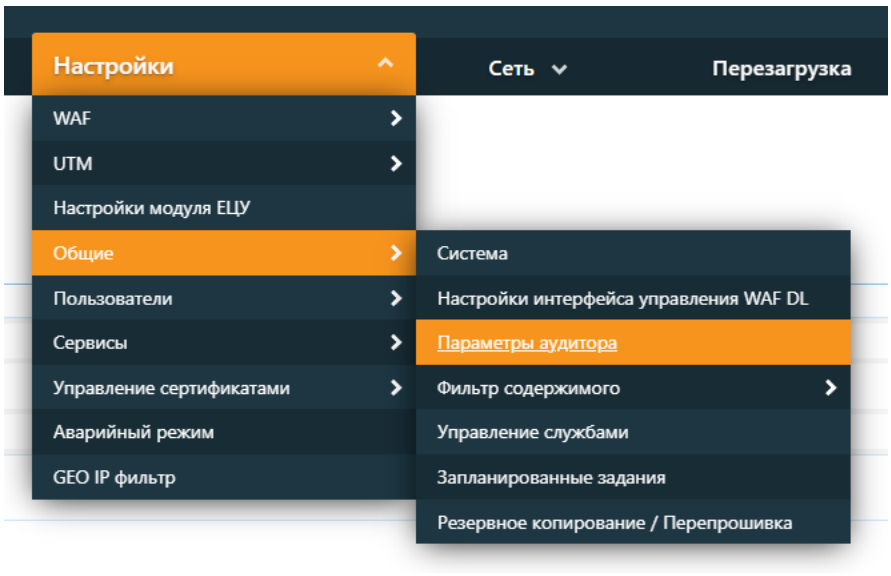


Рисунок 97. Параметры аудитора

Вкладка *Настройка журнала* (см. Рисунок 98) позволяет выбрать какие типы событий безопасности будут заносится в журналы, а также параметры для журналирования на удаленный сервер.

- *Уровень логирования.* Типы событий безопасности в выпадающем списке упорядочены по значимости от наименее значимых в нижних строках списка до «Чрезвычайной ситуации» в верхней строке списка. При выборе типа события, в журналы будут попадать события как с выбранным типом значимости, так и с более высокими. Например, при выборе «ошибка (error)» в журналы будут заноситься типы событий: Ошибка (error), Критическая ситуация (crit), Тревога (alert), Чрезвычайная ситуация (emerg).
- *Протокол внешнего лог-сервера.* Выпадающий список для выбора протокола транспортного уровня (UDP / TCP) для журналирования на удаленный сервер. По умолчанию выбрано значение *Отключить*. При выборе протокола становятся доступны следующие поля:
  - *Адрес внешнего лог-сервера.* Доступен ввод доменного имени сервера или IP-адрес сервера (IPv4 и IPv6).
  - *Порт внешнего лог-сервера.*
  - *Уровень логирования на внешний сервер.* Аналогично выпадающему списку *Уровню логирования.* Значение применяется только для журналирования на удаленный сервер.
- *Включить внешний сервер LEEF.* Чекбокс активирует логирование на удаленный LEEF-сервер. При активации становятся доступны поля:
  - *Адрес внешнего сервера LEEF.* Доступен ввод доменного имени сервера или IP-адрес сервера (IPv4 и IPv6).
  - *Порт внешнего сервера LEEF.*
- *Непрерывная отправка журналов в ЕЦУ.* Чекбокс доступен, если модуль **WAF Dallas Lock** находится в домене безопасности ЕЦУ. Если чекбокс включен, то **WAF Dallas Lock** постоянно отправляет журналов на ЕЦУ. Если отключен, отправка журналов осуществляется по требованию сервера.
- *Уровень логирования ЕЦУ.* Аналогично выпадающему списку *Уровню логирования.* Значение применяется только для журналирования на ЕЦУ.

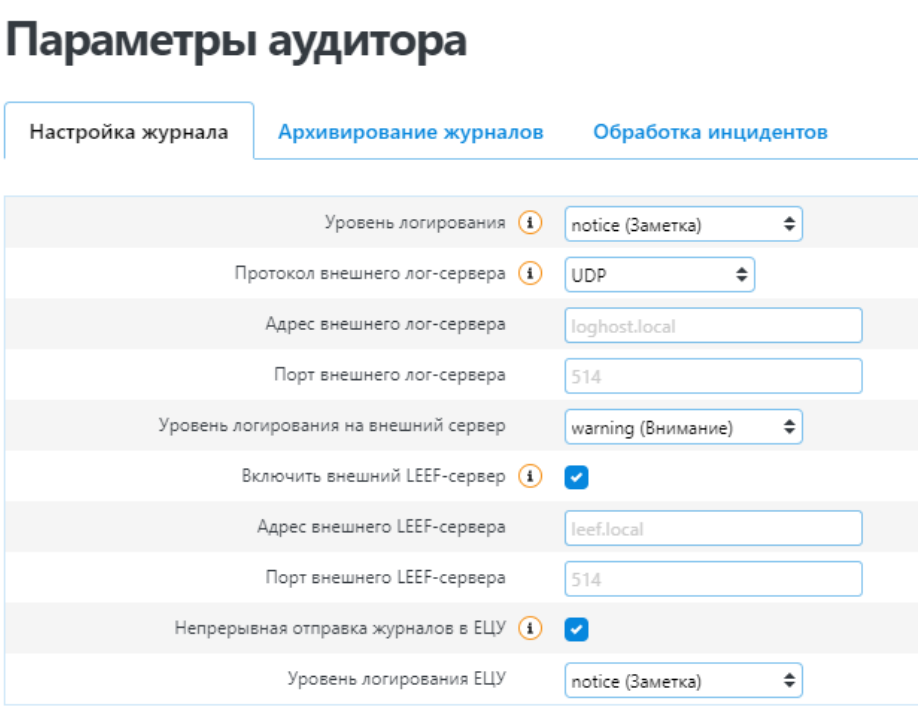


Рисунок 98. Настройка журнала

Вкладка *Архивирование журналов* (см. Рисунок 99) позволяет создать, скачать, загрузить и удалить архивированные журналы.

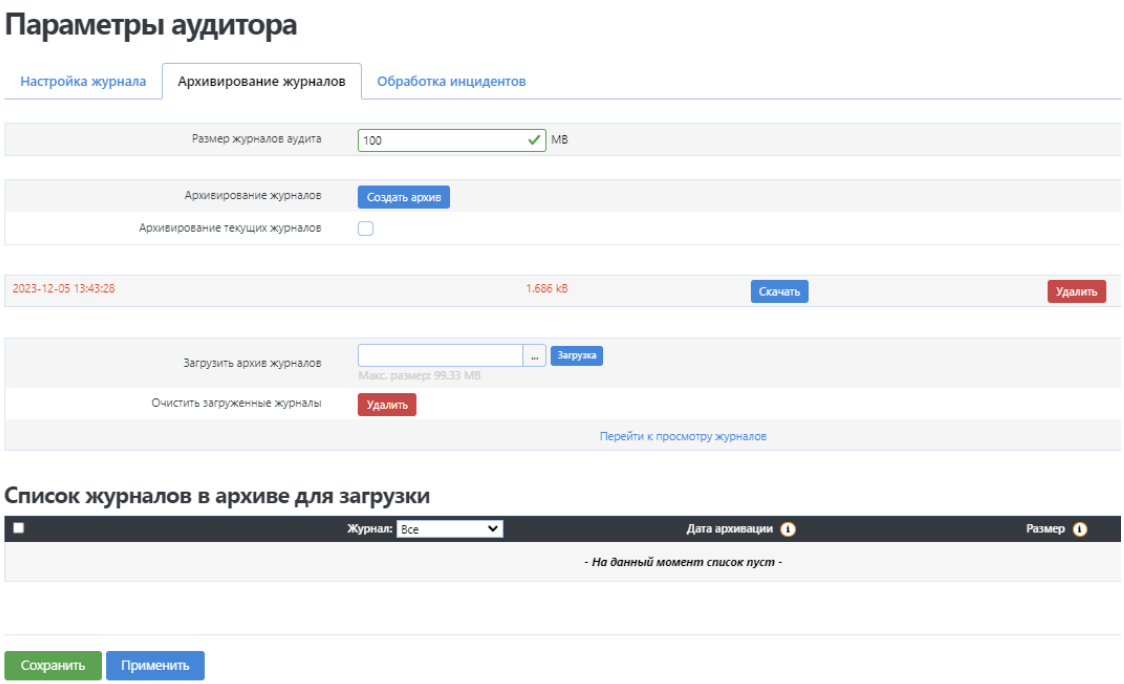


Рисунок 99. Архивирование журналов

На данной странице кнопки ***Создать архив, Скачать, Удалить*** (см. Рисунок 100) имеют «прямой» характер работы, то есть при нажатии, действие будет происходить немедленно, в отличие от «транзакционного» характера работы на других страницах конфигурации.

Вкладка *Архивирование журналов* включает следующие настройки (см. Рисунок 100):

- *Размер журналов аудита*. Поле задает максимальный размер системного журнала;

- *Создать архив*. При нажатии на кнопку создается архив журналов;
- *Архивирование текущих журналов*. Если этот чекбокс включен, то с помощью кнопки *Создать архив* будет создан архив текущей сессии;
- *Скачать*. При нажатии на кнопку происходит скачивание архива с журналами (расширение архива: tar.gz - tar плюс gzip);
- *Удалить*. Удаляет архивированный журнал.
  Архивированные журналы выделяются цветом и имеют следующие настройки (см. Рисунок 100):
  - *Красный цвет*. Указывает, что архивированный журнал не был загружен на компьютер ни одного пользователя;
  - *Зеленый цвет*. Указывает, что архивированный журнал был загружен хотя бы один раз на компьютер пользователя.
  - *Дата и время*. Указывается дата создания архивированного журнала;
  - *Размер файла*. Указывается размер архивированного журнала.

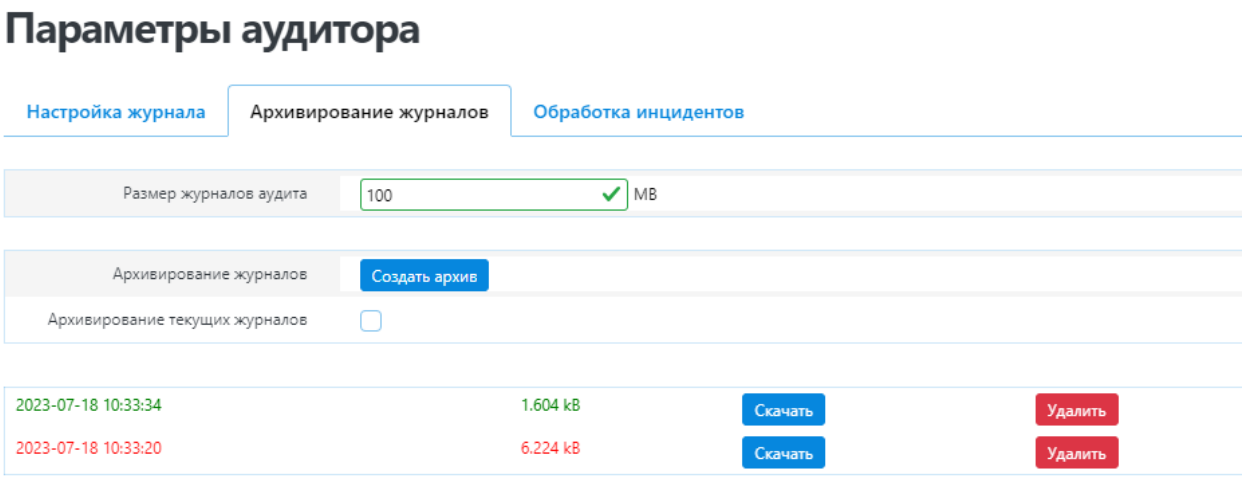


Рисунок 100. Описание особенностей функционала кнопок

Для загрузки архива журналов (см. Рисунок 101):

1. Нажать кнопку **Загрузка**;
2. Выбрать архивированный журнал из архивов журналов на ПК;
3. Нажать кнопку **Загрузить**;
4. В таблице **Список журналов в архиве для загрузки** появятся следующие поля:
   - *Чекбокс*. Для выбора журнала и выполнением над ним действий следует его активировать;
   - *Журнал*. Отображает тип журналов, загруженных из архивированного журнала. Предусмотрена фильтрация по типу журналов;
   - *Дата архивации*. Отображает дату и время создания загруженного журнала;
   - *Размер*. Показывает размер журнала.
5. **Удалить**. Кнопка предназначена для удаления архива из поля *Загрузить архив журналов*.

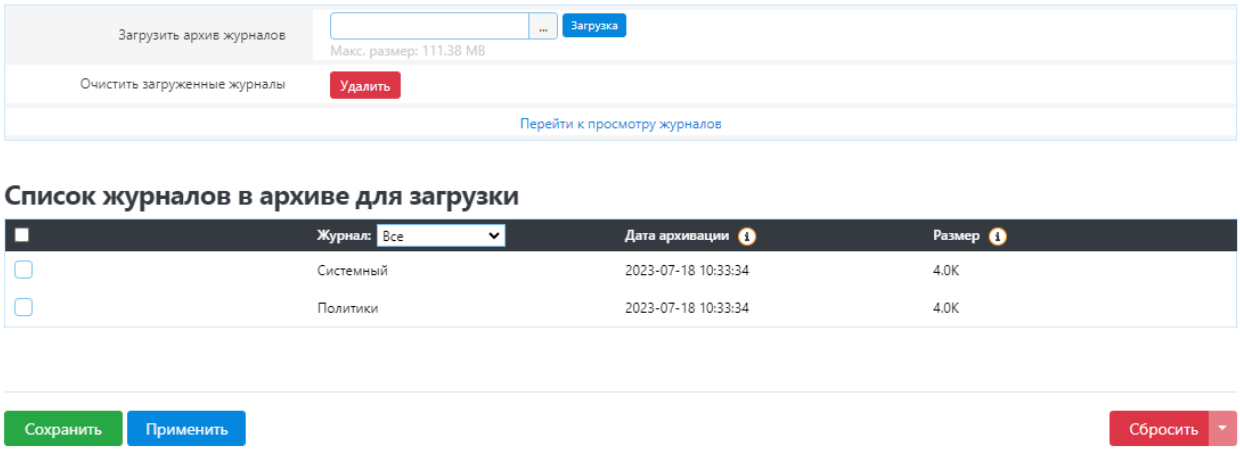


Рисунок 101. Загрузка архивных журналов

Кнопка **Сбросить** удаляет данные из поля *Загрузить архив журналов* и *Список журналов в архиве для загрузки*.
Кнопка **Сохранить** сохраняет введенные настроек в форме веб-интерфейса.
Для применения внесенных изменений необходимо нажать кнопку **Применить**.

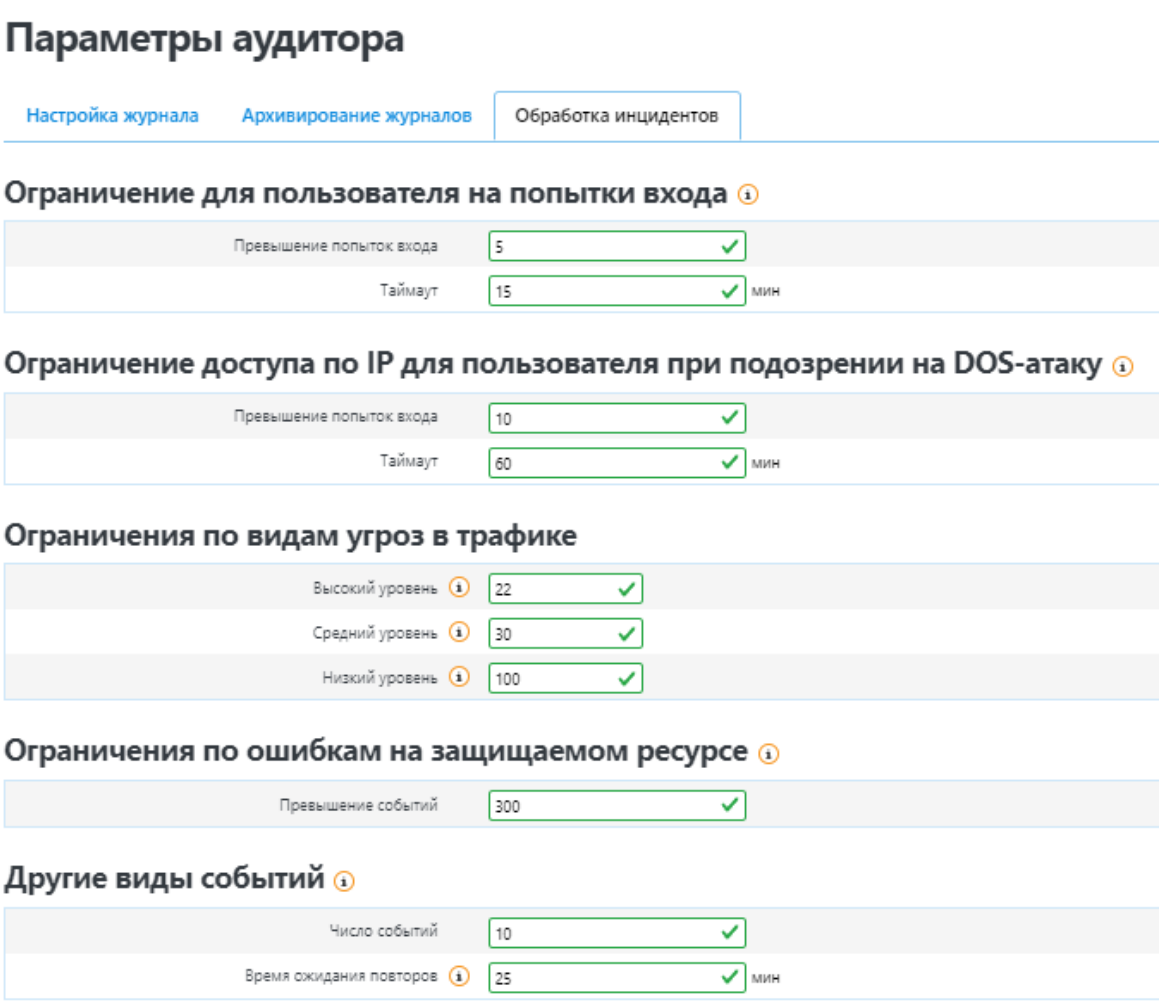


Рисунок 102. Обработка инцидентов

Вкладка *Обработка инцидентов* (см. Рисунок 102) позволяет администратору (root) задать пороговые значения для реакции **WAF Dallas Lock** на инциденты безопасности.

Блок **Ограничение для пользователя на попытки входа.** Содержит настройки для блокировки учетной записи пользователя, при превышении указанного количества попыток входа через интерфейс пользователя.

- *Превышение попыток входа.* Поле задает пороговое значение попыток авторизации пользователя. При превышении этого значения учетная запись будет добавлена в список *Заблокированные пользователи*.
- *Таймаут.* В поле указывается значение времени в минутах. По истечении указанного времени, заблокированная учетная запись будет автоматически удалена из списка *Заблокированные пользователи*.

Блок **Ограничение доступа по IP для пользователя при подозрении на DOS-атаку**. Задает пороговое значение для попыток входа с одного IP-адреса через интерфейс пользователя и протокол SSH.

- *Превышение попыток входа.* Поле задает пороговое значение количества попыток авторизации пользователя с одного IP-адреса. При превышении значения пользователь с данным IP-адресом будет добавлен в список *Заблокированные пользователи*.
- *Таймаут.* В поле указывается значение времени в минутах. По истечении указанного времени заблокированный пользователь будет автоматически удален из списка *Заблокированные пользователи*.

Блок **Ограничения по видам угроз в трафике**. Пороговые значения количества угроз высокого, среднего и низкого уровней. При превышении значений, указанных в полях данного блока, происходить блокировка IP-адреса источника угрозы.

Блок **Ограничения по ошибкам на защищаемом ресурсе**. Содержит поле *Превышение событий,* определяющее пороговое количество ошибок на защищаемом ресурсе, при достижении которого произойдет блокировка IP-адреса источника.

Блок **Другие виды событий**.

- *Число событий.* Поле задает пороговое количество событий одного типа, по достижению которого **WAF Dallas Lock** блокирует IP-адрес источника событий.
- *Время ожидания повторов.* Период времени в минутах, в течение которого отслеживаются события одного типа.

5.4.5 Фильтр содержимого

Страница **Фильтр содержимого** (см. Рисунок 103) позволяет администратору информационной безопасности задать настройки управления параметрами системы обнаружения и предотвращения вторжений. Настроить анализ сетевого трафика на предмет возможных угроз безопасности для защищаемых ресурсов.

Содержит следующие блоки настроек:

- **Настройка количества обслуживающих процессов**. Управление режимами обработки сетевого трафика и настройка количества процессов при инспекции WAF (см. 5.4.5.1 Настройка количества обслуживающих процессов);
- **Настройки переменных фильтра содержимого**. Содержит поля, определяющие IP-адреса серверов различных сервисов, по которым будет идти трафик (веб-сервер, почтовый север, sql-сервер). Задается уровень эвристического анализа (см.

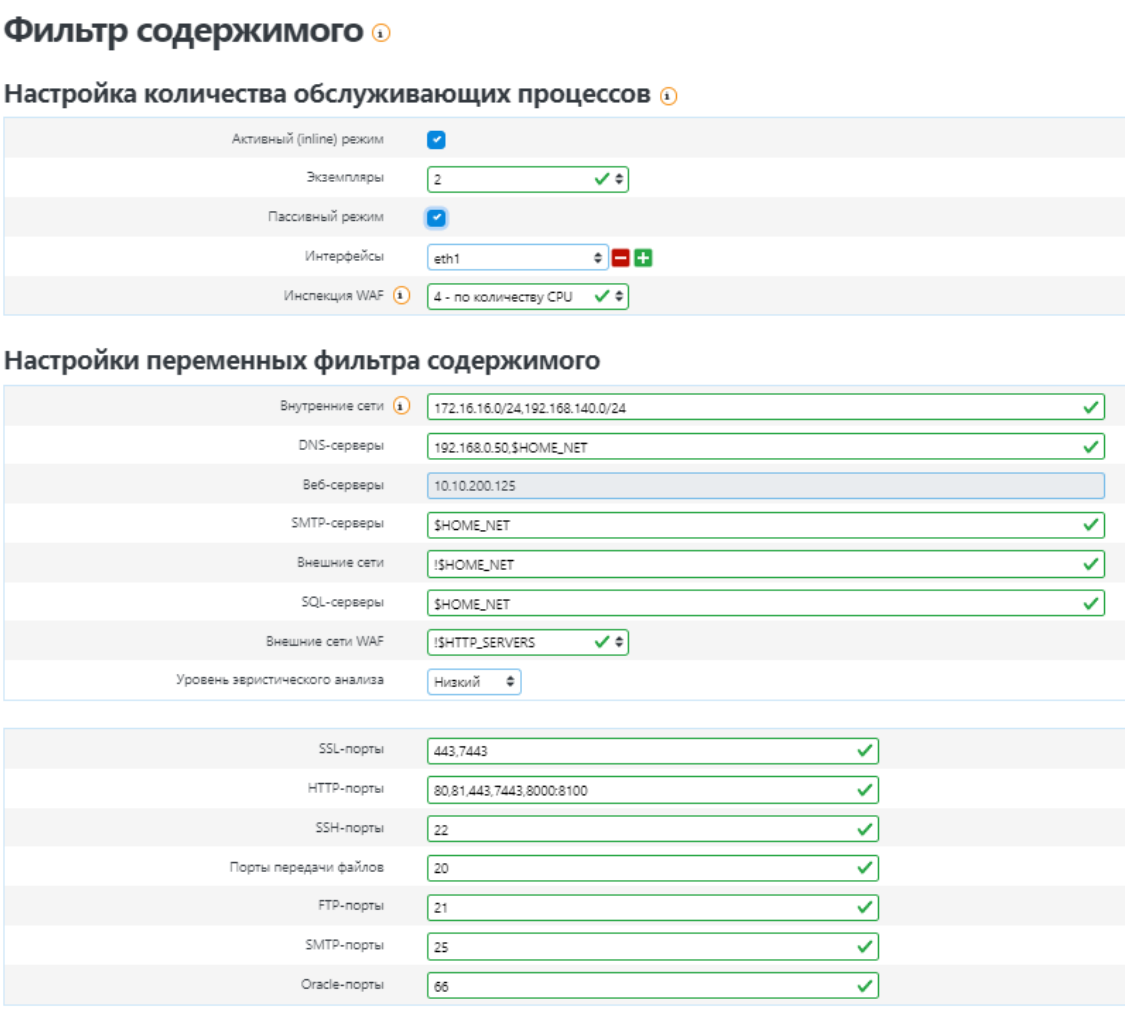


Рисунок 103. Фильтр содержимого

5.4.5.1 Настройка количества обслуживающих процессов

Данный блок настроек включает следующие параметры (см. Рисунок 103):

- *Активный (inline) режим.* При включении параметра, система обнаружения и предотвращения вторжений активно вмешивается в сетевой трафик, блокируя или модифицируя пакеты в соответствии с правилами безопасности. Режим использует модуль ядра Netfilter для перенаправления трафика перед тем, как пакеты достигнут своего назначения, что может вносить определенную задержку и увеличивать нагрузку на систему. В данном режиме осуществляется немедленная защита от потенциальных угроз. Однако, при использовании необходимо проявлять осторожность, так как возможны ложные срабатывания, которые могут привести к блокировке легитимного трафика;
- *Экземпляры***.** Поле доступно после включения Активного (inline) режима. Позволяет настраивать количество процессов/экземпляров контекстного фильтра, которые будут запущены для обработки трафика и будут работать в активном режиме;
- *Пассивный режим***.** При включении параметра, система обнаружения и предотвращения вторжений не блокирует трафик, а только информирует о потенциальных угрозах безопасности. Режим подходит для мониторинга сетевой активности;
- *Интерфейсы.* Поле доступно после включения Пассивного режима. Позволяет выбрать сетевые интерфейсы, через которые будет проходить трафик в пассивном режиме. На каждый интерфейс запускается отдельный процесс контекстного фильтра;

Комбинация активного и пассивного режимов. Например, возможность использование активного (inline) режима для блокировки известного вредоносного трафика, в то время как параллельный экземпляр в пассивном режиме используется для более детального анализа трафика и обнаружения более сложных атак.

Пассивный и активный режимы контекстного фильтра не имеют встроенной функциональной возможности расшифровки сетевого трафика.

- *Инспекция WAF.* Параметр позволяет выбрать количество процессов, которые будут использоваться в связке с прокси-сервером при инспекции WAF;
- *Инспекция UTM SSL***.** Параметр позволяет выбрать количество процессов, которые будут использоваться в связке с прокси-сервером при инспекции UTM.

Прокси-сервер использует ключи для расшифровки зашифрованных пакетов данных, позволяя контекстному фильтру анализировать содержимое этих пакетов для обнаружения угроз безопасности.

5.4.5.2 Настройки переменных фильтра содержимого

Данный блок настроек включает следующие параметры (см. Рисунок 103):

- *Внутренние сети.* Поле содержит IP-адреса защищаемых внутренних сетей и задает переменную $HOME_NET;
- *DNS-серверы.* Поле содержит IP-адреса DNS-серверов в вашей сети и задает переменную $DNS_SERVERS. По умолчанию принимает значение $HOME_NET;
- *Веб-серверы.* Поле содержит IP-адреса веб-серверов в вашей сети и задает переменную $HTTP_SERVERS. По умолчанию принимает значение $HOME_NET;
- *SMTP-серверы.* Поле содержит IP-адреса почтовых серверов в вашей сети, которые используют протокол SMTP для отправки и получения электронной почты и задает переменную $SMTP_SERVERS. По умолчанию принимает значение $HOME_NET;
- *Внешние сети.* Поле содержит IP-адреса внешних сетей и задает переменную $EXTERNAL_NET, которая используется для правил UTM. По умолчанию принимает значение !$HOME_NET (все значения, кроме $HOME_NET);
- *SQL-серверы.* Поле содержит IP-адреса серверов баз данных SQL и задает переменную $SQL_SERVERS. По умолчанию принимает значение $HOME_NET;
- *Внешние сети WAF.* Поле содержит IP-адреса внешних сетей и задает переменную $WAF_NET, которая используется для правил WAF. По умолчанию принимает значение !$HTTP_SERVERS (все значения, кроме $HTTP_SERVERS);.
- *Уровень эвристического анализа*: Параметр определяет, насколько глубоко устройство будет анализировать трафик для обнаружения угроз. Может быть выбрано одно из трех значений (по умолчанию — низкий):
    - Низкий — низкое количество ложных срабатываний, низкое количество обнаруженных сканирований;
    - Средний — сбалансированный режим между низким и высоким уровнями;
    - Высокий — высокое количество ложных срабатываний, высокое количество обнаруженных сканирований.
- *SSL-порты.* Порты, на которые контекстный фильтр будет ожидать SSL-трафик. По умолчанию принимает значение 443,7443;
- *HTTP-порты.* Порты, на которые контекстный фильтр будет ожидать HTTP-трафик. По умолчанию в WAF принимает значение 80, 81, 443, 7443, 8000:8100;
- *SSH-порты.* Порты, на которые контекстный фильтр будет ожидать SSH-трафика. По умолчанию принимает значение 22;

- *Порты передачи файлов.* Порты, на которые контекстный фильтр будет ожидать трафик передачи файлов. По умолчанию принимает значение 20;
- *FTP-порты.* Порты, на которые контекстный фильтр будет ожидать FTP-трафик. По умолчанию принимает значение 21;
- *SMTP-порты.* Порты, на которые контекстный фильтр будет ожидать SMTP-трафик. По умолчанию принимает значение 25;
- *Oracle-порты.* Порты, на которые контекстный фильтр будет ожидать трафик от серверов баз данных Oracle. По умолчанию принимает значение 66.

Кнопка **Сбросить** служит для очистки полей. При нажатии кнопки **Применить** происходит запись введенных настроек в соответствующие config-файлы. При нажатии кнопки **Сохранить** происходит сохранение введенных настроек в форме веб-интерфейса.

5.4.6 Управление службами

На данной странице (см. Рисунок 104) возможно включить или выключить установленные скрипты, инициализация которых происходит при старте системы. Изменения вступят в силу после перезагрузки устройства. Список служб представлен в таблице 4.

Таблица 4. Список служб

Служба	Описание
syslog-ng	Служба, отвечающая за систему журналирования
dnsmasq	Служба, отвечающая за разрешение доменных имен
dropbear	Служба, отвечающая за доступ по SSH (если включен в настройках)
firewall	Служба, отвечающая за реинициализацию правил межсетевого экранирования уровня сети
network	Служба, отвечающая за реинициализацию сетевых интерфейсов
mosquitto	Служба, отвечающая за обмен сообщениями между устройствами, используя службу MQTT
octopus	Служба, отвечающая за сервис кластера
wafuccd	Служба, отвечающая за взаимодействие с ЕЦУ
odhcpd	Служба, отвечающая за работу DHCP и IPv6
cron	Служба, отвечающая за запуск запланированных задач
uhttpd	Служба, отвечающая за веб-интерфейс
uproxy	Служба, отвечающая за режим UTM, предполагающий использование нескольких методов защиты и анализа трафика сети
keepalived	Служба, реализующая протокол VRRP, предназначенный для создания механизма резервирования маршрутизаторов
collectd	Служба, отвечающая за сервис сбора статистики для информационной панели
ctf	Служба, отвечающая за агента анализа трафика
wproxy	Служба, отвечающая за агента анализа трафика и терминации SSL
smartd	Служба, отвечающая за отслеживание работоспособности жесткого диска
watchcat	Служба, отвечающая за работу сторожевого таймера

sysntpd	Служба, отвечающая за получение меток времени

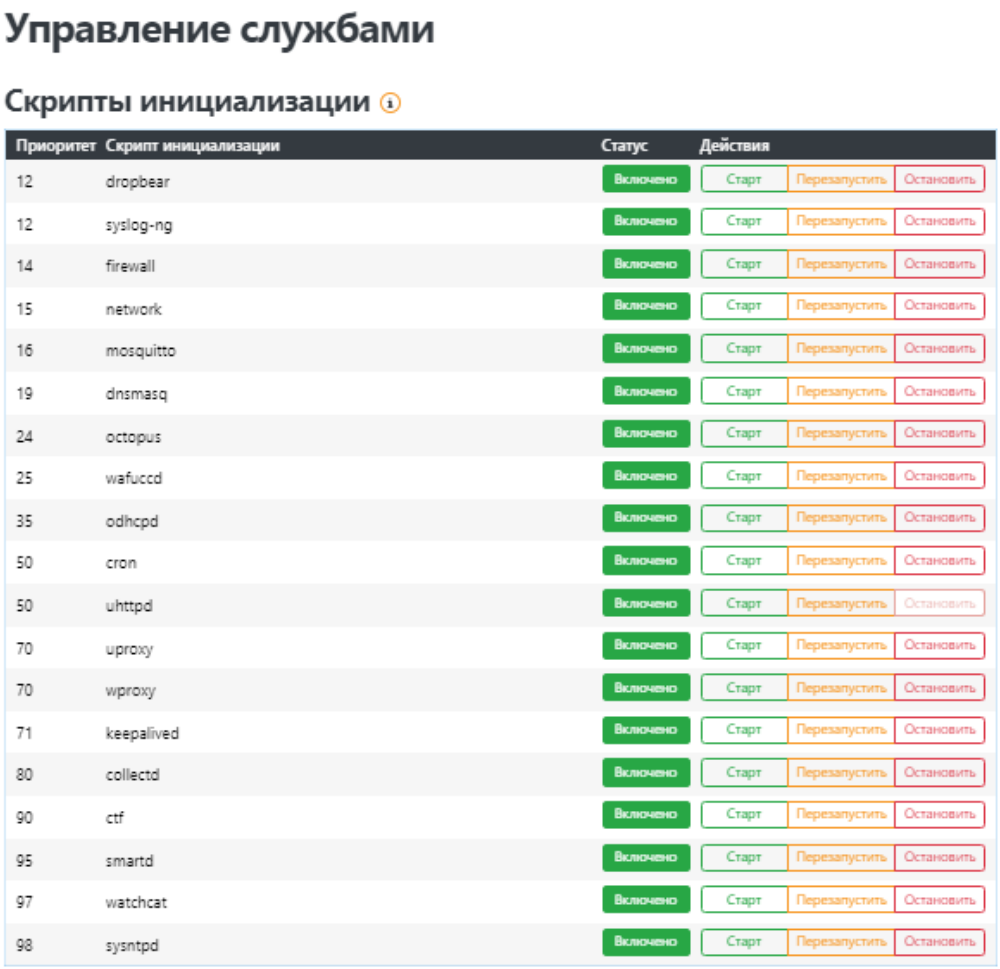


Рисунок 104. Скрипты инициализации

Если выключить один из основных скриптов инициализации (например, «network»), устройство может оказаться недоступным.

5.4.7 Запланированные задания

Данная страница (см. Рисунок 105) позволяет администратору системы создать и применить собственное задание.

Необходимо вручную перезапустить службу *cron*, если этот файл был пустым перед внесением изменений.

Рисунок 105. Запланированные задания

5.4.8 Резервное копирование и перепрошивка

Данная страница (см. Рисунок 106) позволяет администратору создать архив текущих конфигурационных настроек **WAF Dallas Lock**, восстановить конфигурационные настройки из ранее сохраненного архива.

На данной странице отсутствуют стандартные для других страниц кнопки **Сохранить, Применить, Отменить.** Кнопки **Создать архив, Восстановить, Установить** и **Сбросить** имеют «прямой» характер работы, то есть при нажатии действие будет происходить немедленно, в отличие от «транзакционного» характера работы на других страницах конфигурации.

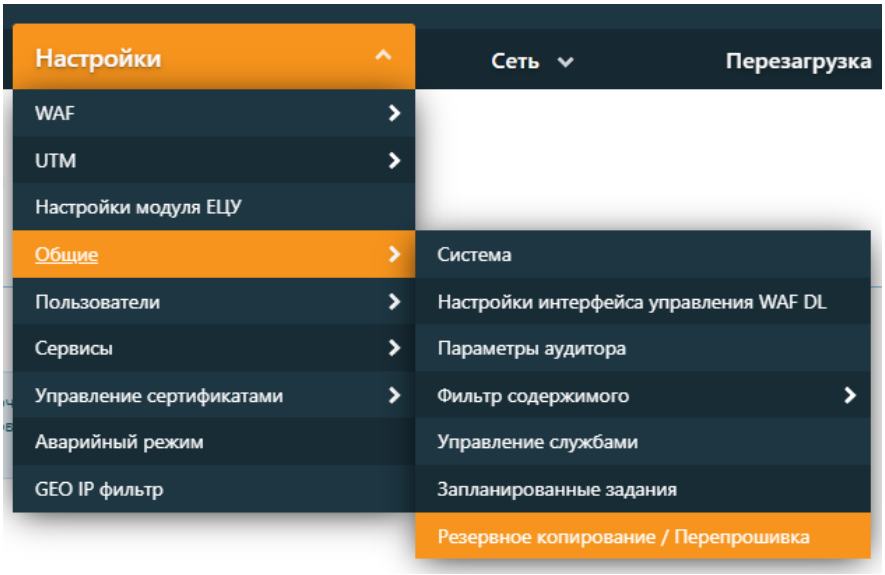


Рисунок 106. Резервное копирование/Перепрошивка

Вкладка *Действия* (см. Рисунок 107). При нажатии кнопки **Создать архив** в блоке **Резервное копирование** создается архив с текущими конфигурационными настройками системы.

Восстановить резервную копию. Позволяет восстановить конфигурационные настройки системы. Для этого необходимо нажать кнопку **Восстановить** и выбрать ранее созданный архив конфигурационных настроек системы.

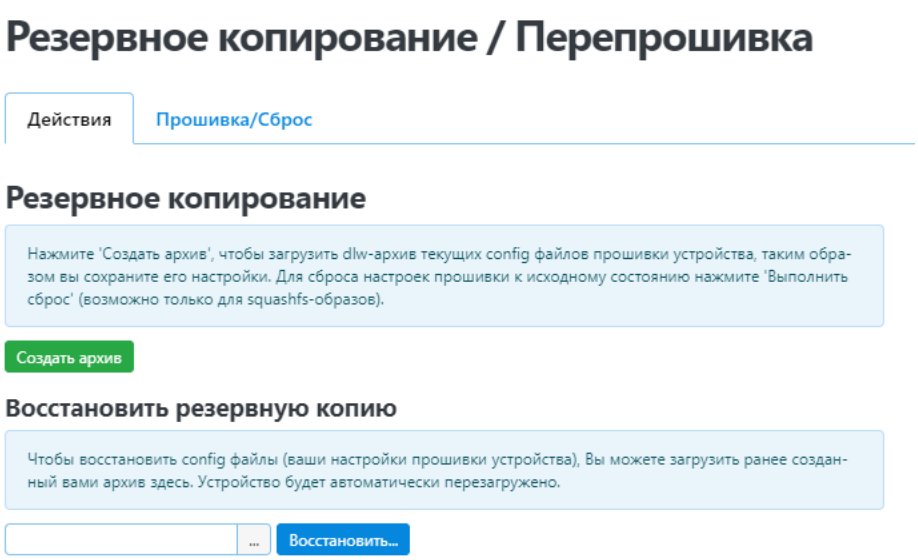


Рисунок 107. Резервное копирование/Перепрошивка

Вкладка *Прошивка/Сброс* (см. Рисунок 108) Блок **Установить новый образ прошивки** позволяет заменить текущую прошивку на новую. Для этого необходимо нажать кнопку **Установить** и выбрать заранее сохраненный на устройство, новый образ прошивки. Поставьте чекбокс *Сохранить настройки* для того, чтобы сохранить текущие конфигурационные настройки системы.

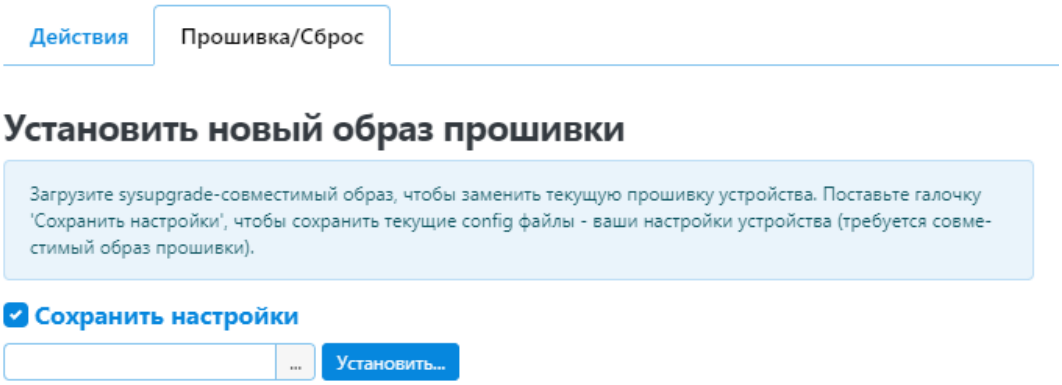


Рисунок 108. Образ прошивки

Блок **Сброс к заводским настройкам** (см. Рисунок 109). Позволяет сбросить **WAF Dallas Lock** к заводским настройкам. Для этого необходимо нажать кнопку **Сбросить**.

Нажатие кнопки *Сбросить* приведет к полному удалению текущих настроек WAF Dallas Lock.
URL по умолчанию: https://192.168.1.1:7443/
При сбросе на заводские настройки доступ к веб-интерфейсу WAF Dallas Lock возможен только с компьютера, находящегося в локальной вычислительной сети.

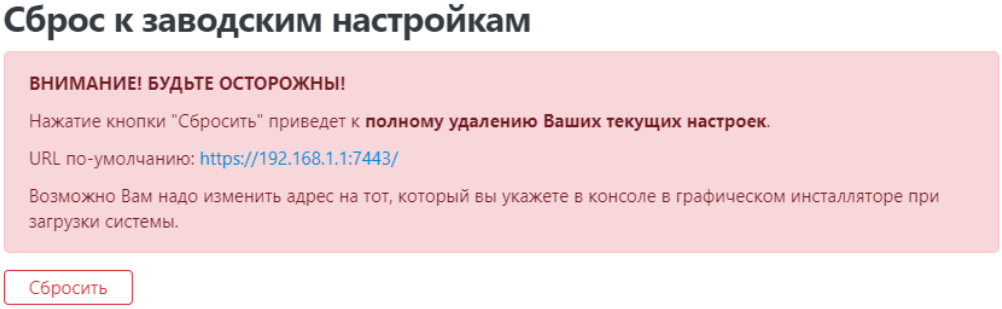


Рисунок 109. Сброс к заводским настройкам

5.5 Настройка пользователей

Данная страница (см. Рисунок 110) позволяет создавать, удалять, менять учетные записи пользователей, использующиеся для доступа к веб-интерфейсу **WAF Dallas Lock**.

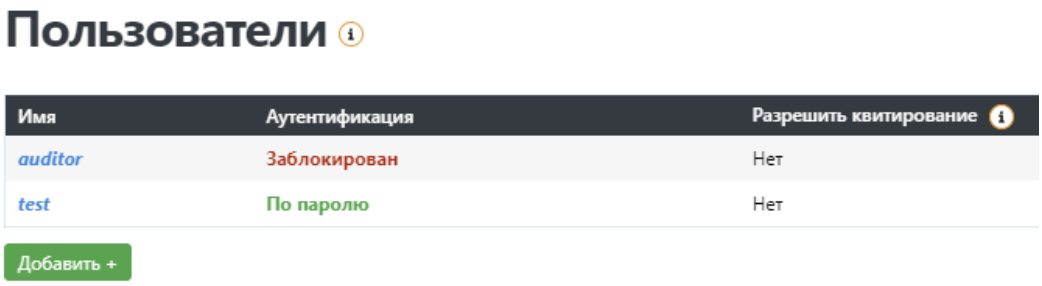


Рисунок 110. Список пользователей

Меню **Пользователи** содержит список учетных записей и доступно только администратору системы. Администратор может создавать пользователей и назначать им отдельные права на аудит и настройку веб-интерфейса. Администратор обладает неограниченными правами и имеет полный доступ ко всем функциям веб-интерфейса.

Для создания нового пользователя системы необходимо вызвать форму добавления пользователя (см. Рисунок 111) кнопкой **Добавить**. В данной форме можно задать следующие параметры:

- имя пользователя;
- пароль;
- аутентификацию пользователя в систему (по паролю, без пароля, заблокирован);
- разрешить или запретить пользователю менять пароль, или принудительно поменять пароль при первом входе в систему;
- добавить в группу пользователей;
- разрешить или запретить квитирование (подтверждение событий инцидентов);
- задать права на просмотр всех или определенных журналов;
- задать права на редактирование всех или определенных настроек системы.

Для редактирования существующего пользователя, нажать кнопку **Изменить**. Для удаления существующего пользователя кнопку **Удалить**.

Из-за особенностей устройства WAF Dallas Lock, у администратора нет возможности создать учетную запись аудитора с именем *audit*. Это происходит из-за того, что при создании учетной записи она помещается в группу audit.

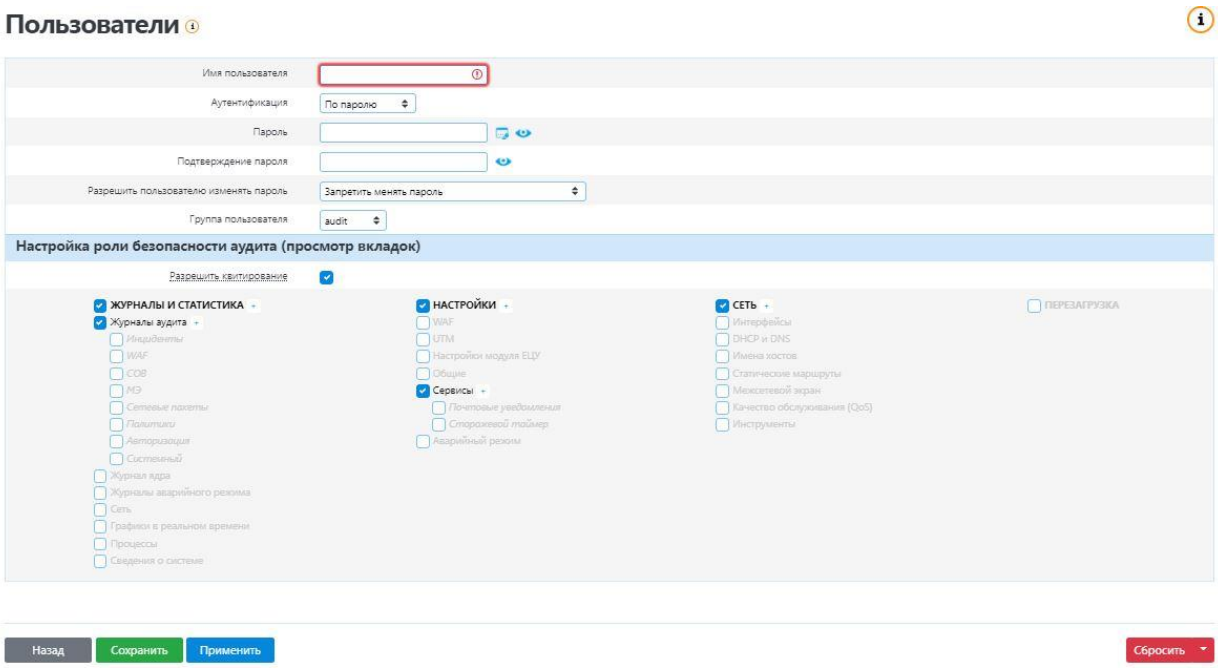


Рисунок 111. Форма добавления пользователя

Заблокированные пользователи

Для просмотра списка заблокированных учетных записей пользователей **WAF Dallas Lock** перейти на страницу **Настройки > Пользователи > Заблокированные пользователи** (см. Рисунок 112).

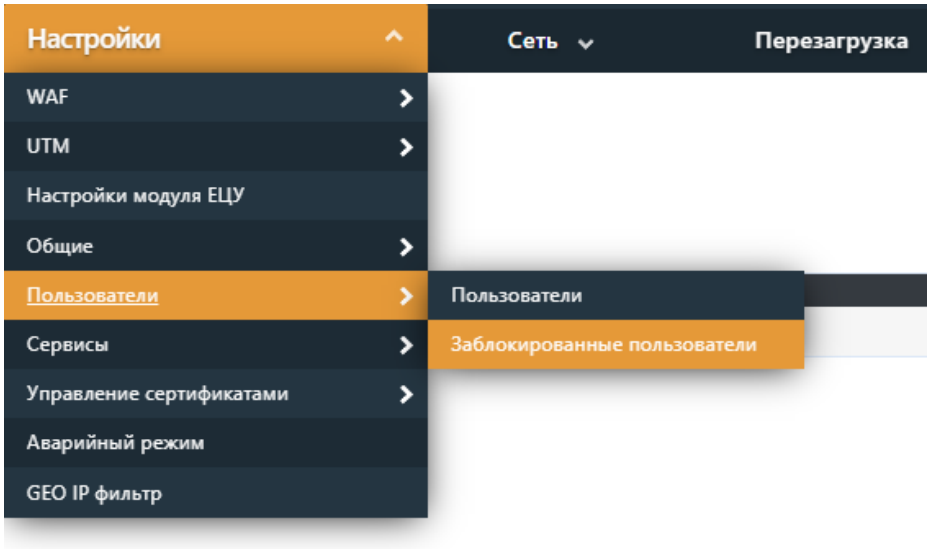


Рисунок 112. Страница «Заблокированные пользователи»

Здесь отображаются заблокированные системой учетные записи пользователей вследствие неправильного ввода пароля несколько раз.

Разблокировка учетной записи пользователя осуществляется автоматически по истечении указанного времени блокировки или после явной разблокировки администратором в разделе **Заблокированные пользователи** (см. Рисунок 113). В таком случае у пользователя появляется возможность осуществить вход в систему снова.

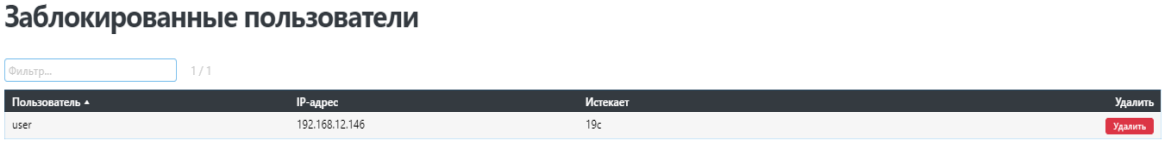


Рисунок 113. Список заблокированных пользователей

Для разблокирования конкретной учетной записи необходимо выбрать ее из списка *Заблокированные пользователи* и нажать на кнопку **Удалить**.

5.6. Настройка сервисов

5.6.1 Настройка почтовых уведомлений

WAF Dallas Lock позволяет настроить уведомление администратора об обнаруженных атаках по электронной почте (см. Рисунок 114).

Протокол. Можно выбрать один из протоколов передачи почты (SMTP, TLS/SSL, STARTTLS).

Имя сервера. Необходимо указать имя почтового сервера пользователя.

Порт. Указать порт для передачи почты.

Авторизация. Если в настройках почты необходимо задать данные для авторизации пользователя почты от куда будет идти отправка уведомлений для этого необходимо поставить чекбокс *Авторизация* и ввести авторизационные данные в строках *Имя пользователя* и *Пароль.*

В строках *Имя отправителя* и *Имя получателя* указывается адрес почты с которой будет отправляться уведомления и куда соответственно.

Для проверки введенных данных, нажмите кнопку **Применить** *и* **проверить**, после этого будет отправлено тестовое письмо.

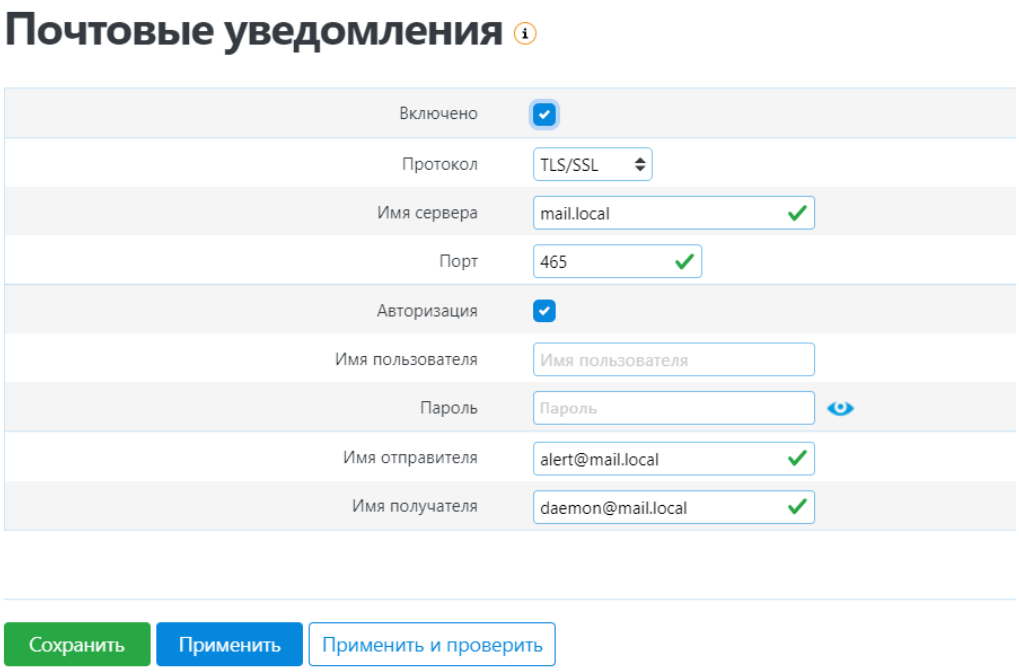


Рисунок 114. Настройка почтовых уведомлений

5.6.2 Настройка сторожевого таймера

Сторожевой таймер позволяет настроить периодичную перезагрузку **WAF Dallas Lock** или перезагрузку при потере интернет-соединения на определенное администратором время (см. Рисунок 115).

Режим работы. Можно выбрать перезагрузку при потере интернет-соединения или настроить периодичную.

Задержка принудительной перезагрузки. При перезагрузке системы сторожевой таймер вызовет программную перезагрузку. Ввод ненулевого значения, вызовет отложенную аппаратную перезагрузку, если программная перезагрузка не удастся. Чтобы включить программную перезагрузку в строке нужно ввести количество секунд. Если стоит значение «0», значит задержка принудительной перезагрузки будет отключена.

Период. В периодическом режиме это значение задает период перезагрузки. В режиме перезагрузки

при потере Интернет-соединения данное значение определяет максимальный период времени без доступа в Интернет, после которого устройство перезагружается. По умолчанию значение в секундах, можно использовать суффикс «m» для указания минут, «h» — часов, «d» — дней.

Хост пинг-запроса. В данной строке указывается адрес хоста для пинг-запроса.

Период пинг-запроса. В данной строке указывается временной интервал проверки Интернет-соединения. По умолчанию значение в секундах. Используется суффикс «m» для указания минут, «h» — часов, «d» — дней.

Период сетевой недоступности должен быть больше, чем период проверки доступности сети. Период проверки доступности сети не может быть меньше минуты. Период сетевой недоступности не может быть меньше двух минут.

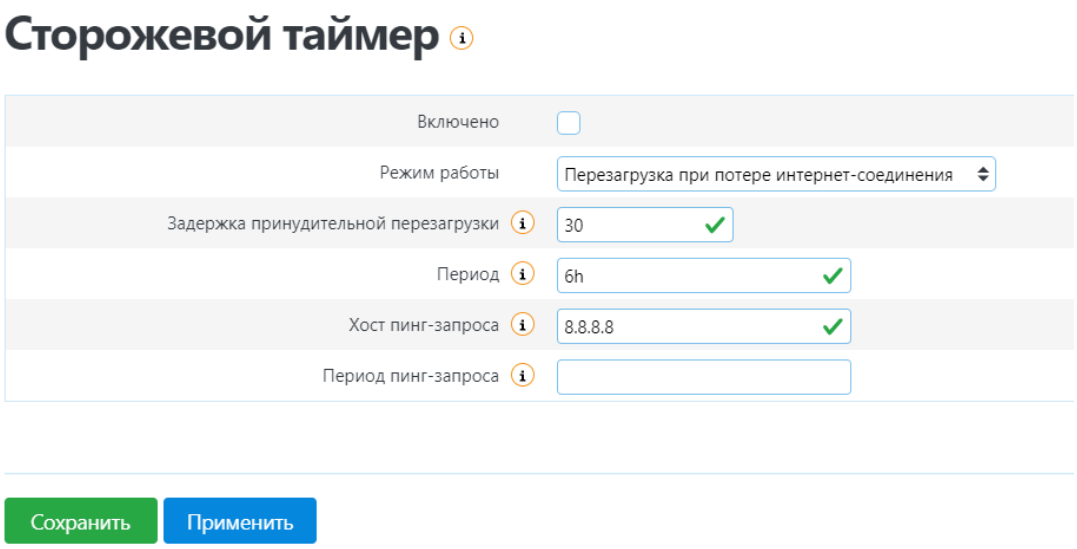


Рисунок 115. Настройка сторожевого таймера

5.7 Управление сертификатами

WAF Dallas Lock использует защищенный протокол HTTPS для управления устройством, может перехватывать и дешифровывать транзитный трафик пользователей, передаваемый по протоколу SSL (HTTPS), а так же может производить авторизацию администраторов в веб-интерфейс управления на основе их сертификатов.

5.7.1 Серверные сертификаты

На данной вкладке (см. Рисунок 116) имеется список серверных сертификатов в системе для защищаемых узлов. В строке *Сгенерировать сертификат* можно создать самоподписаный сертификат для защищаемого сервера/хоста или добавить уже готовый сертификат ранее сгенерированный сторонним УЦ.

Для создания самоподписанного сертификата необходимо указать имя защищаемого узла, количество дней действия сертификата, выбрать размер ключа и нажать кнопку **Сгенерировать**.

Для того чтобы добавить защищаемый ресурс со сгенерированным сертификатом, нужно нажать на имя сертификата в списке сертификатов или нажать на ссылку *Перейти к защищаемым ресурсам.* В строке *Добавить защищаемый ресурс* выбрать из списка сгенерированный сертификат и нажать кнопку **Добавить**.

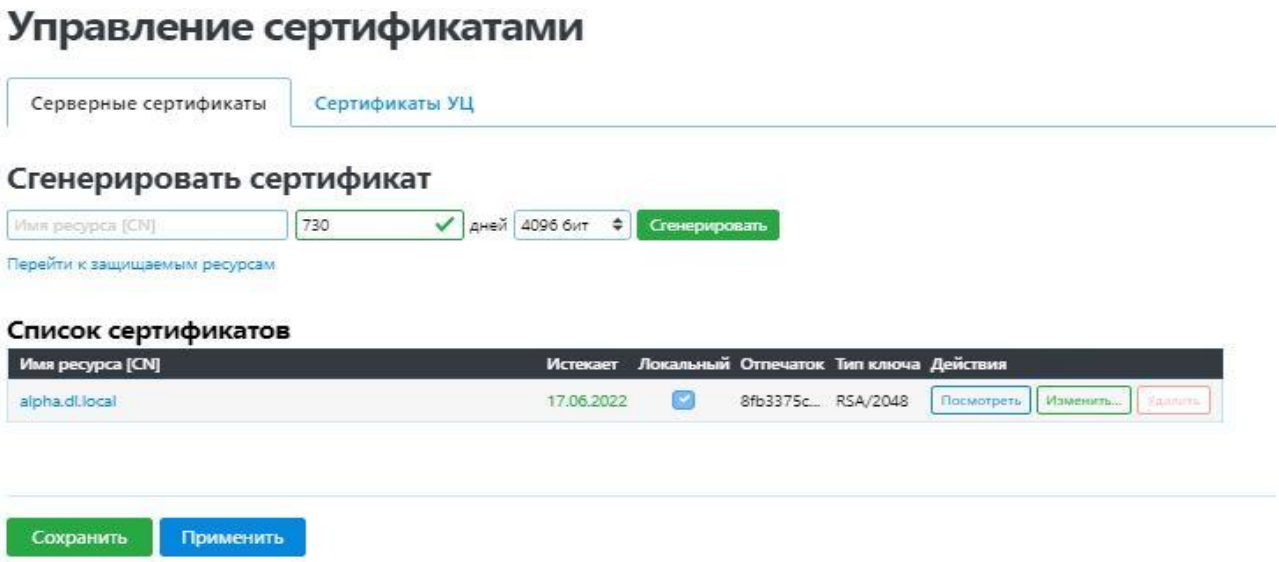


Рисунок 116. Список защищаемого узла и сертификатов

Для того чтобы добавить сертификат стороннего УЦ необходимо нажать на ссылку *Перейти к защищаемым ресурсам* (см. Рисунок 117). В строке *Загрузить новый сертификат* необходимо выбрать сертификат стороннего УЦ с расширениями (*.pem, *.crt, *.cert), который содержит приватный ключ и сертификат.

Кнопка **Посмотреть** служит для просмотра информации о субъекте и объекте сертификата.

Кнопка **Изменить** служит для обновления срока действия сертификата или изменения длины ключа.

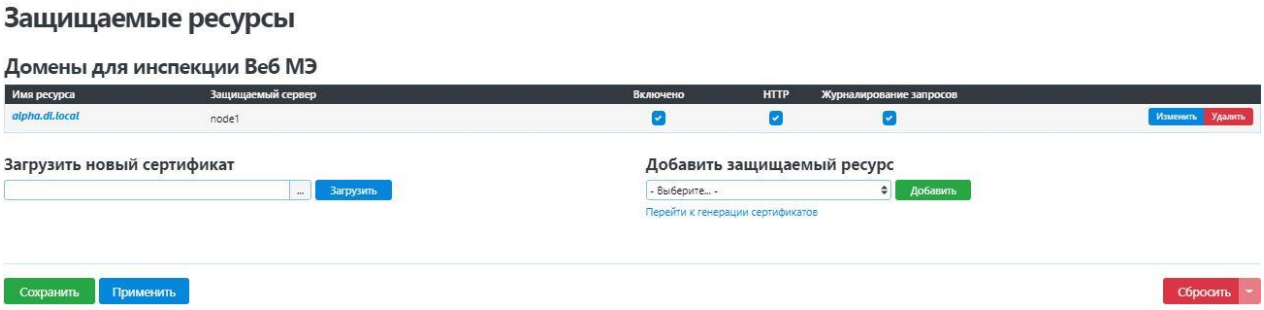


Рисунок 117. Добавление защищаемого узла и сертификата

5.7.2 Сертификаты УЦ

На данной вкладке (см. Рисунок 118) имеется список сгенерированных самоподписанных локальных сертификатов УЦ (CA cert).

Настройки заголовков сертификатов. Данные настройки используются в качестве заголовков при генерации любого из самоподписанных сертификатов внутренним УЦ.

По умолчанию созданы следующие сертификаты:

- CA Root WAF DL основной сертификат УЦ в системе. Им подписан серверный сертификат для авторизации в интерфейсе WAF Dallas Lock по протоколу HTTPS. (более подробно в разделе

При резервном копировании конфигурации **WAF Dallas Lock** сохраненные ключи аутентификации SSH не сохраняются и требуют повторного импорта на **WAF Dallas Lock.**

- 5.4.2.2 Web-интерфейс).
- CA VHost WAF DL промежуточный сертификат УЦ (intermediate CA) для создания самоподписанных серверных сертификатов.
- CA UTM WAF DL промежуточный сертификат УЦ (intermediate CA) для перехвата HTTPS-трафика пользователей к внешним защищаемым ресурсам. Служит для контроля

исходящего трафика.

Сертификаты можно заменить на сгенерированные внешним доверенным УЦ добавив его в строке *Добавить дополнительный сертификат,* после этого он отобразится *в* списке **Дополнительные сертификаты.**

Кнопка **Посмотреть** служит для просмотра информации о субъекте и издателе сертификата.

Кнопка **Скачать** служит для экспорта сертификата на компьютер.

Кнопка **Изменить** служит для обновления срока действия сертификата или изменения длины ключа.

Важно отметить, что сертификаты, подписанные сторонними УЦ известны веб-браузерам. Самоподписанные сертификаты необходимо импортировать в хранилище доверенных сертификатов веб-браузера вручную. Поскольку соединения с доменами, обслуживаемыми такими сертификатами по умолчанию блокируются.

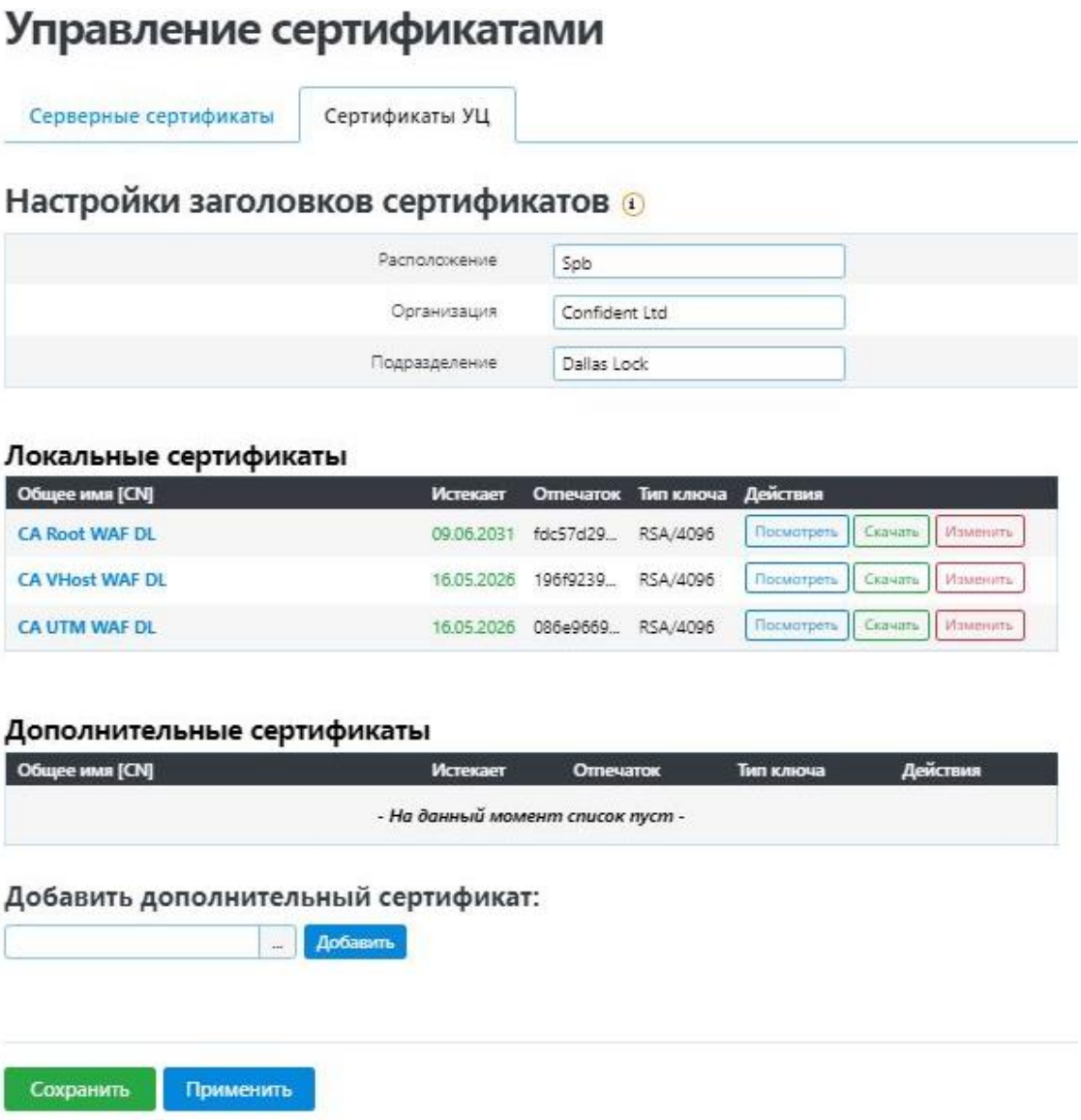


Рисунок 118. Локальные сертификаты

5.8 Настройка аварийного режима

При переводе устройства в аварийный режим работы происходит блокировка всего проходящего информационного потока (трафика), кроме информационного потока для управления **WAF Dallas Lock** и передачи данных на ЕЦУ. Для этого происходит остановка всех сервисов, кроме сервисов из заранее определенного «белого» списка.

Управление WAF Dallas Lock может осуществляться через веб-интерфейс или по протоколу SSH,

доступ осуществляется по умолчанию со всех адресов. Для обеспечения доступа с определенных адресов необходимо явно указать их в пункте меню **Сеть > Межсетевой экран > Списки доступа** (подробно в разделе 6.5.5 Списки доступа МЭ). В этом же пункте меню можно задать доступ к устройству только с адресов локальной сети, в которой находится **WAF Dallas Lock**.

Каждый переход в аварийный режим сопровождается записью в журнале аварийного режима и журнале **Инциденты**. На странице **Журнала аварийного режима** производится запись о последнем переходе системы в аварийный режим.

5.8.1 Список сбоев

В список сбоев/прерываний входят:

- Превышение занятого места на локальном носителе (диске) свыше установленного порогового значения. Значение задается в пункте меню **Аварийный режим** (см. Рисунок 119). Параметрами по умолчанию являются: 80% занятого дискового пространства для извещения пользователя о заканчивающемся дисковом пространстве, 90% для перехода в аварийный режим.
- Нарушение контроля целостности (КЦ) всех запрещенных к модификации объектов программной части **WAF Dallas Lock**.
- Невозможность запуска сервиса из контролируемого списка.
- Перевод в аварийный режим администратором устройства.

Контроль целостности запрещенных к модификации объектов программной части WAF Dallas Lock проводится администратором устройства вручную в пункте меню **Аварийный режим** при старте системы, а также в автоматическом режиме службой *cron* с периодичностью в один час.

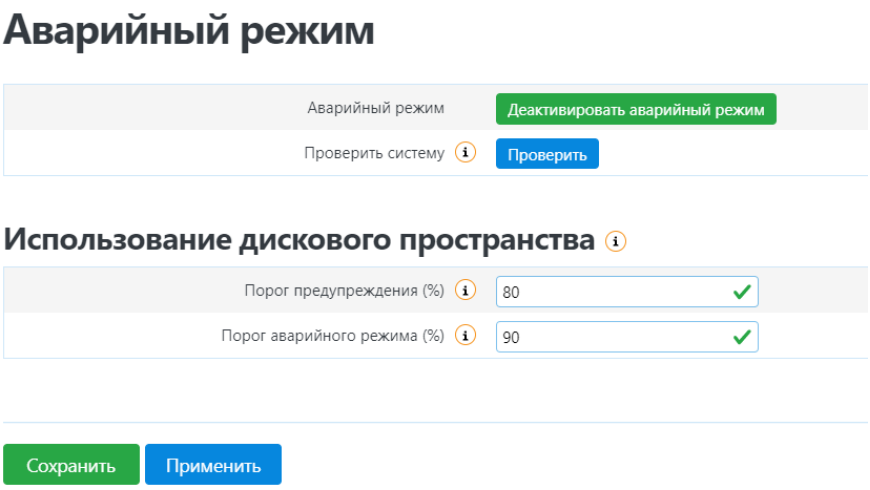


Рисунок 119. Аварийный режим

5.8.2 Возвращение к нормальному режиму работы

Для восстановления (возврата) к штатному состоянию WAF Dallas Lock по списку сбоев необходимо выполнить следующие действия:

- При превышении порогового значения занятого места на диске произвести операцию архивирования журналов, при которой создается архив всех журналов устройства, появляется возможность сохранить журналы на локальный носитель, при этом все журналы очищаются. Выход из аварийного режима будет произведен автоматически.
- При нарушении КЦ произвести сброс **WAF Dallas Lock** к заводским настройкам или загрузить новый образ прошивки. При этом устройство перезагрузится и войдет в нормальный режим работы.
- При невозможности запуска сервиса из контролируемого списка произвести загрузку ранее сохраненного файла настроек (при этом выход из аварийного режима произвести вручную, через соответствующий пункт меню), сбросить **WAF Dallas Lock** к заводским настройкам или загрузить новый образ прошивки (см. раздел 5.4.8 Резервное копирование и перепрошивка).

- Если перевод в аварийный режим был выполнен администратором устройства, то выход из аварийного режима произвести вручную.

При восстановлении штатной работы **WAF Dallas Lock** все сервисы и правила восстанавливаются до нормального (безопасного) состояния.

5.9 GEO IP фильтр

WAF Dallas Lock позволяет настроить доступ к защищаемому ресурсу из определенных стран по геолокации на основе IP-адреса (см. Рисунок 120).

- *Фильтр.* Поле для фильтрации по стране или континенту в списках стран.
- *Сбросить.* Кнопка очистки поля *Фильтр*.
- *Проверить обновления.* Кнопка обновляет значения в списках стран.
- *Автоматически.* При активации чекбокса обновление стран в списках стран будет происходить в автоматическом режиме.
- *Запретить трафик из стран.* Список стран, из которых запрещен трафик.
- *Разрешить.* Кнопка для разрешения трафика из страны, название которой находится в первом столбце в строке с данной кнопкой.
- *Разрешить трафик из стран.* Список стран, из которых разрешен трафик.
- *Запретить.* Кнопка для запрета трафика из страны, название которой находится в первом столбце в строке с данной кнопкой.
- *Разрешить все.* Кнопка перемещает все страны в список *Разрешить трафик из стран.*
- *Запретить все.* Кнопка перемещает все страны в список *Запретить трафик из стран.*
- Для применения новых настроек, нажмите кнопку **Применить**.

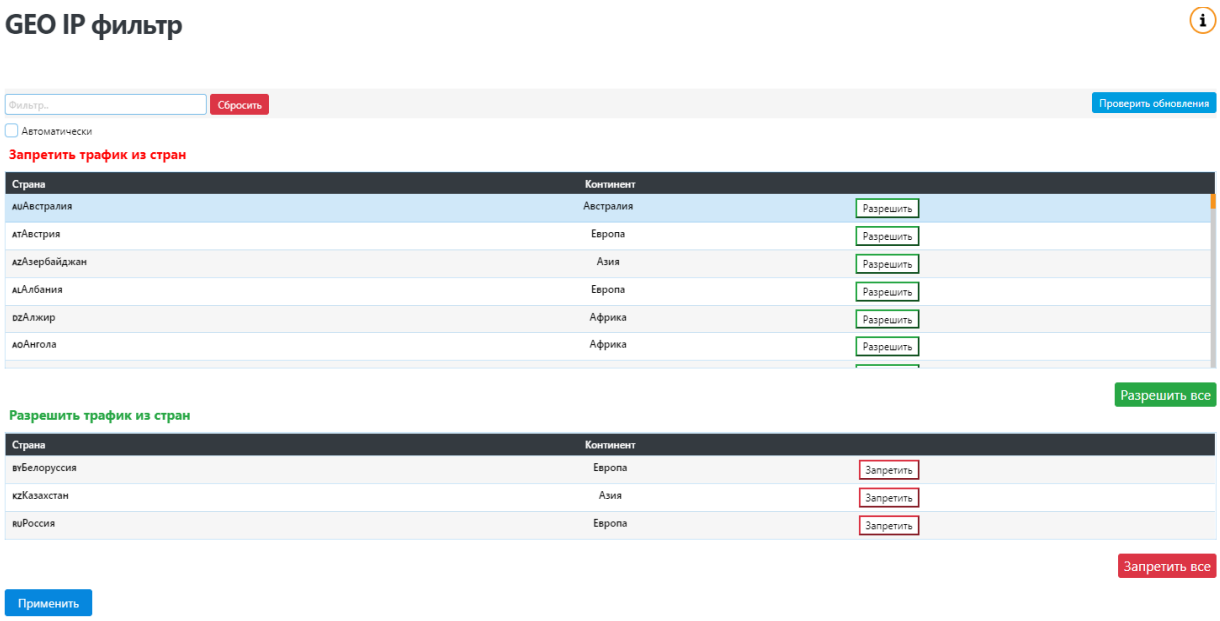


Рисунок 120. GEO IP фильтр

6 СЕТЬ

Для детального описания сети, в которую был интегрирован **WAF Dallas Lock**, а также для создания пользовательских правил безопасности, существует раздел **Сеть**. Также раздел отображает данные о состоянии сети и сетевых интерфейсов LAN, IPv4 WAN, IPv6 WAN и DMZ.

Для перехода к разделу необходимо в основном меню консоли выбрать вкладку **Сеть**. Пункт меню **Сеть** не имеет своей страницы и при нажатии на данный пункт происходит открытие списка меню второго уровня (см. Рисунок 121).

Данный раздел содержит следующие страницы:

- интерфейсы;
- DHCP и DNS;
- имена хостов;
- статические маршруты;
- межсетевой экран;
- качество обслуживания (QoS);
- диагностика.

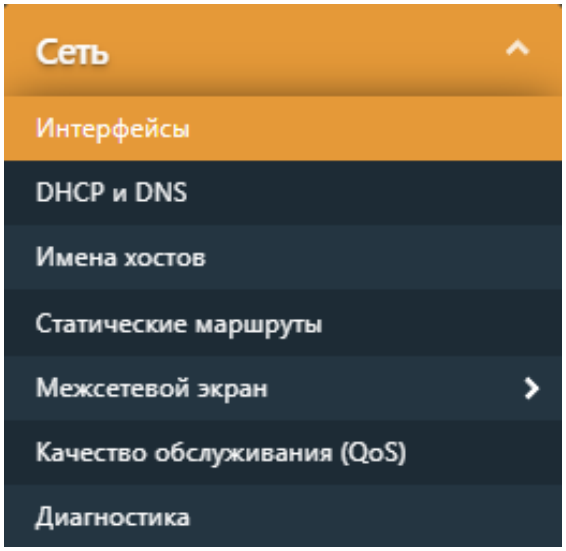


Рисунок 121. Сеть

6.1 Интерфейсы

На данной странице можно настроить сетевые интерфейсы LAN, IPv4 WAN, IPv6 WAN, DMZ (см. Рисунок 122). Для объединения нескольких интерфейсов в мост необходимо выбрать опцию *Объединить в мост* и ввести список интерфейсов, разделенных пробелами.

После добавления и настройки нового интерфейса требуется перезагрузка **WAF Dallas Lock**. Без перезагрузки новый интерфейс не будет запущен.

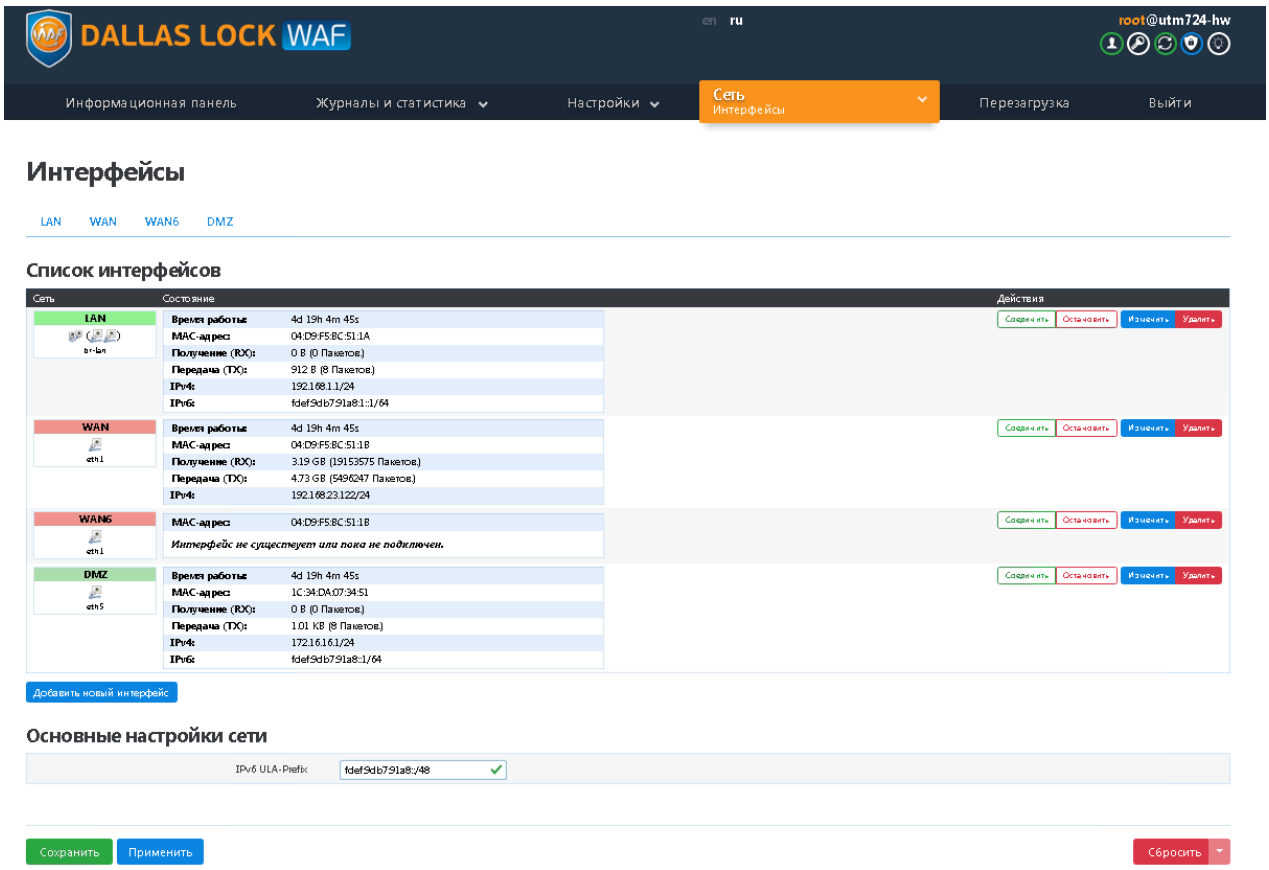


Рисунок 122. Интерфейсы

Для каждого вида интерфейса доступна своя вкладка с одноименным названием. У каждого интерфейса существуют четыре категории настроек: *Основные настройки, Дополнительные настройки, Настройка канала, Настройка межсетевого экрана.*

На вкладке интерфейса LAN, в категории *Основные настройки* (см. Рисунок 123), можно увидеть текущее состояние интерфейса, а также указать основные настройки.

В строке *Протокол* можно указать способ получения адреса интерфейса, выбрав из основных:

- Статический адрес (указание вручную).
- DHCP-клиент (получение адреса автоматически с DHCP-сервера в сети IPv4).
- Неуправляемый (если используется неуправляемое коммутационное оборудование и указывается лишь MAC-адрес).
- IPv6 в IPv4 (RFC4213) (настроенное туннелирование IPv6 через IPv4: метод для создания туннелей точка-точка путем инкапсуляции пакетов IPv6 внутри заголовков IPv4, чтобы передавать их по маршрутизации IPv4 инфраструктуры по стандарту RFC4213).
- IPv6 через IPv4 (6to4) (механизм перехода IPv6 6to4).
- IPv6 через IPv4 (6rd) (механизм перехода IPv6 6RD).
- DHCPv6-клиент (получение адреса автоматически с DHCP-сервера в сети IPv6).

Для того чтобы сменить режим работы интерфейса, например, со Статический адрес на DHCP-клиент, необходимо выбрать DHCP-клиент и нажать кнопку **Изменить протокол**. После указания протокола отобразятся соответствующие выбранному способу настройки интерфейса.

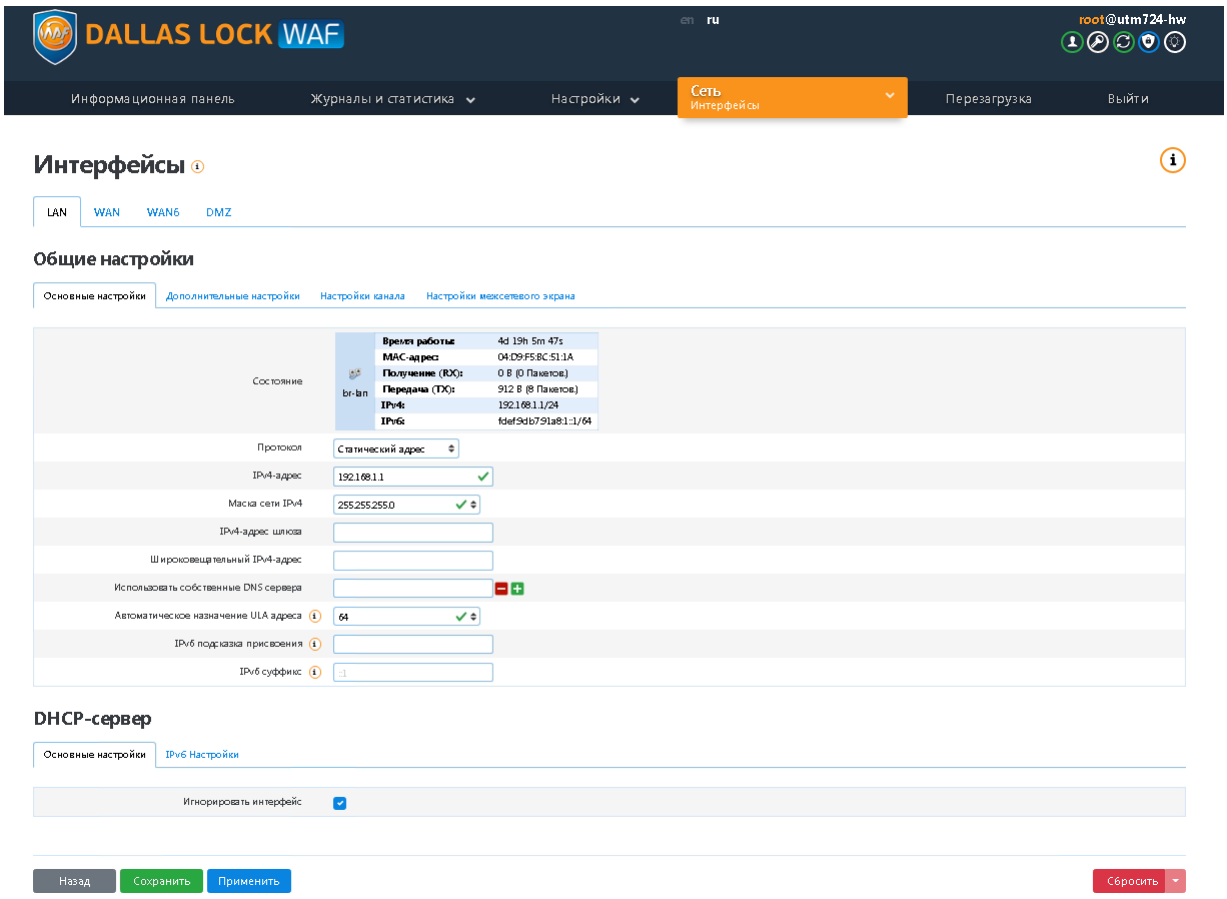


Рисунок 123. LAN – Основные настройки

Во вкладке для интерфейса LAN, в категории *Дополнительные настройки* (см. Рисунок 124), можно выбрать настройки:

- *Запустить при загрузке* (автоматическое включение интерфейса при запуске **WAF Dallas Lock** — по умолчанию включен). Если отключить эту опцию, то при сохранении и применении настроек данный интерфейс будет выключен. Аналогичная опция есть в дополнительных настройках для всех интерфейсов.
- *Использовать встроенный IPv6-менеджмент* (использование сервиса IP-management — IPAM). Для указанных настроек активация произойдет после проставления отметки напротив названия.
- Также можно указать необходимый *MAC-адрес* (по умолчанию принимает значение MAC-адреса интерфейса).
- Указать *размер MTU* (максимальный размер полезного блока данных одного пакета), по умолчанию принимает значение 1500.
- *Использовать метрику шлюза* (метрика — это значение, назначаемое IP-маршруту для определенного сетевого интерфейса, определяющего стоимость использования этого маршрута), по умолчанию принимает значение 0.

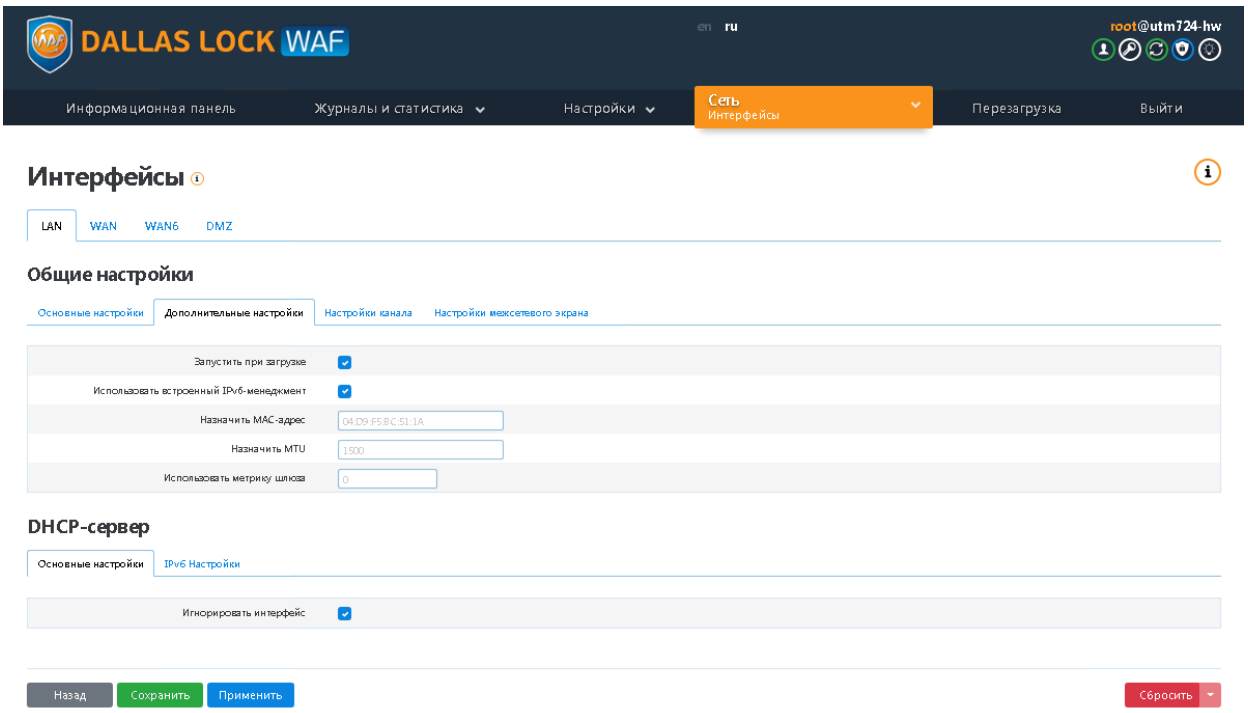


Рисунок 124. LAN – Дополнительные настройки

На вкладке для интерфейса LAN, в категории *Настройки канала* (см. Рисунок 125), можно выбрать настройки объединения в мост для указанных интерфейсов. Существует также возможность включить протокол STP (сетевой протокол (или семейство сетевых протоколов), предназначенный для автоматического удаления циклов (петель коммутации) из топологии сети на канальном уровне в Ethernet-сетях).

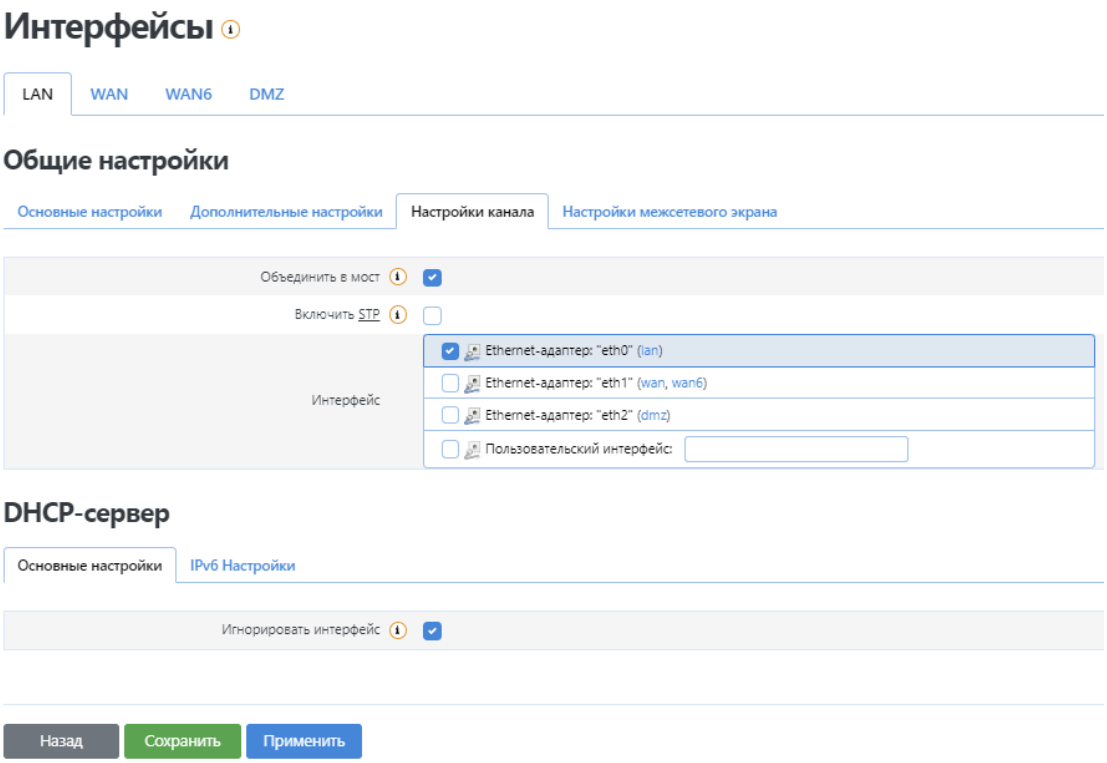


Рисунок 125. LAN – Настройки канала

На вкладке для интерфейса *LAN*, в категории *Настройки межсетевого экрана* (см. Рисунок 126), можно выбрать зону межсетевого экрана, в которую необходимо добавить настраиваемый

интерфейс. Для исключения интерфейса из зон межсетевого экрана, необходимо выбрать пункт *Не определено*, либо заполнить поле *Создать* для добавления новой зоны межсетевого экрана и добавления настраиваемого интерфейса в новую зону.

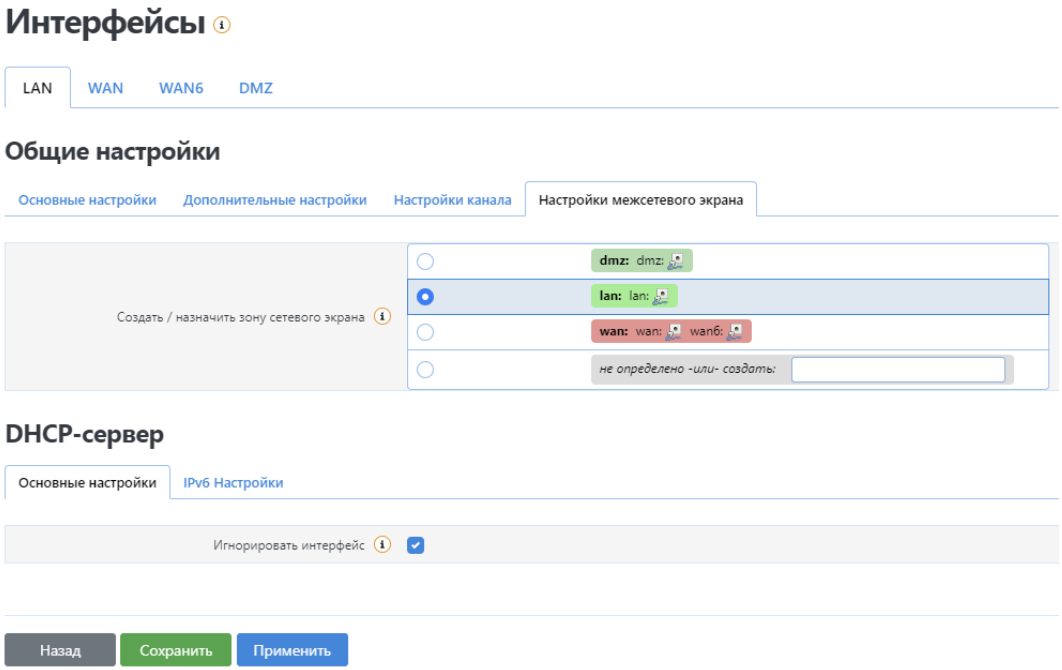


Рисунок 126. LAN – Настройки межсетевого экрана

Аналогичные настройки доступны для остальных интерфейсов, за исключением специализированных настроек.

На вкладке для интерфейса WAN (IPv4 WAN), в категории *Основные настройки* (см. Рисунок 127), можно увидеть текущее состояние интерфейса, а также указать основные настройки для интерфейса.

Для того чтобы сменить режим работы интерфейса, например, со Статический адрес на DHCP-клиент, необходимо в строке *Протокол* вместо Статический адрес, выбрать DHCP-клиент и нажать кнопку **Изменить протокол**. После указания Протокола отобразятся соответствующие выбранному способу настройки интерфейса.

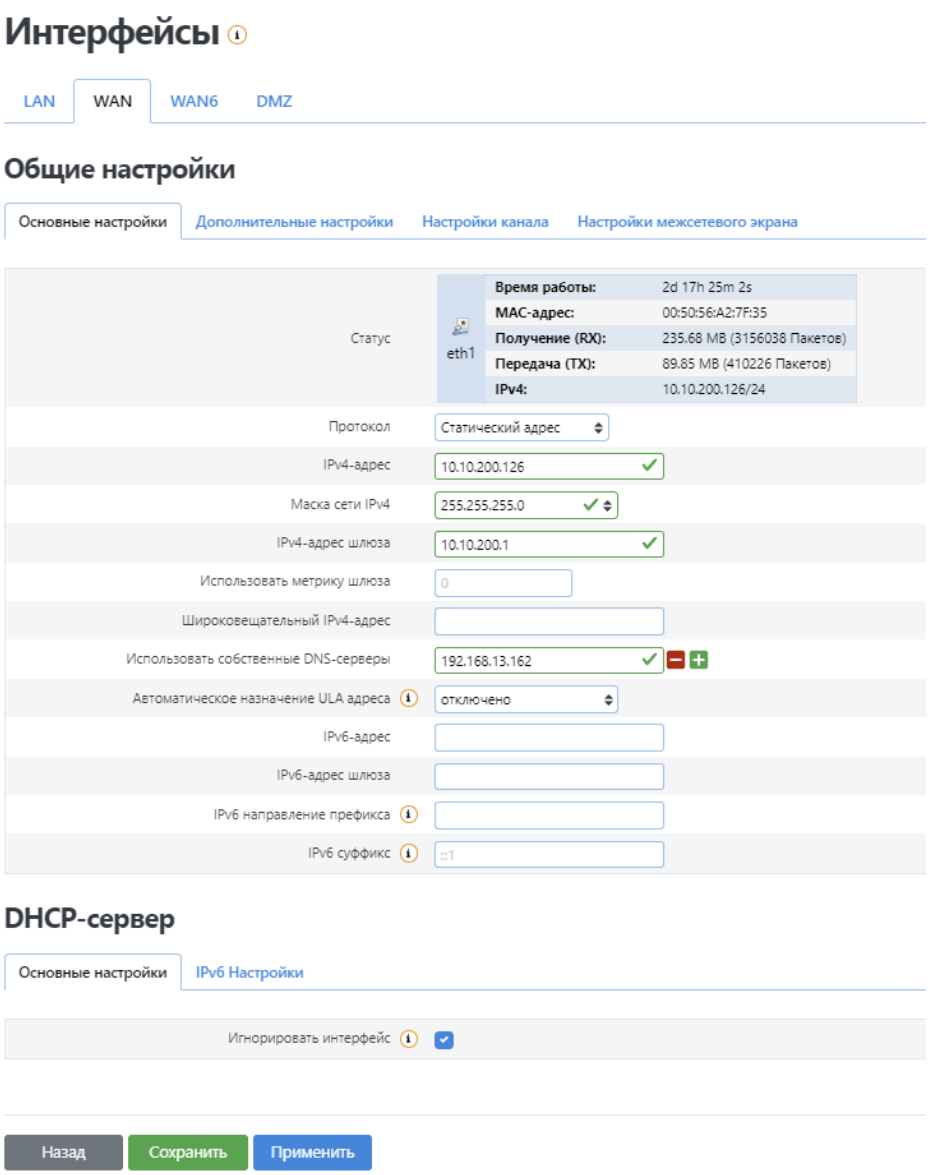


Рисунок 127. WAN – Основные настройки

На вкладке для интерфейса *WAN6 (IPv6 WAN)*, в категории *Основные настройки* (см. Рисунок 128), можно увидеть текущее состояние интерфейса, а также указать основные настройки для интерфейса.

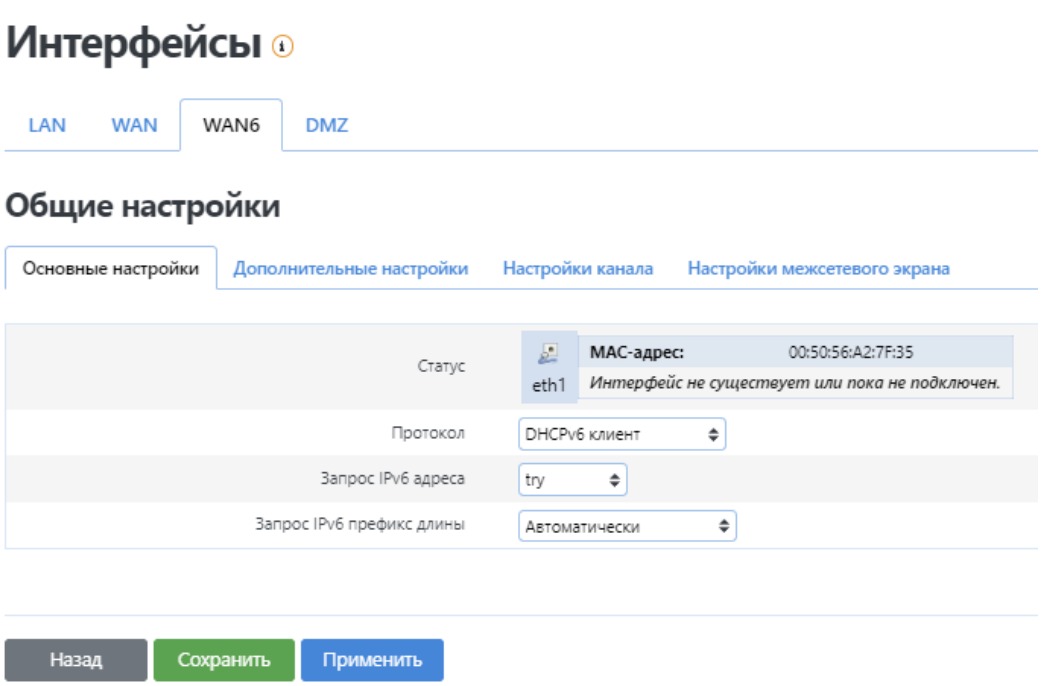


Рисунок 128. WAN6 – Основные настройки

На вкладке для интерфейса *DMZ (Demilitarized Zone)*, в категории *Основные настройки* (см. Рисунок 129), можно увидеть текущее состояние интерфейса, а также указать основные настройки для интерфейса.

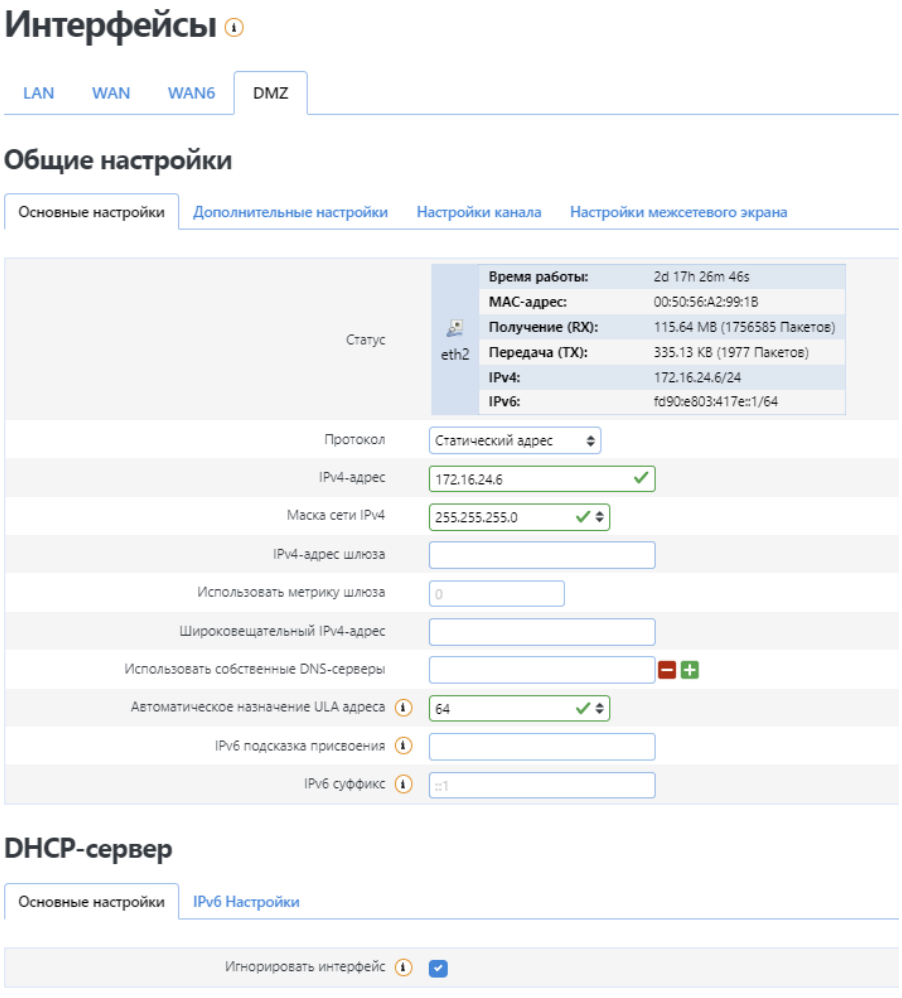


Рисунок 129. DMZ – Основные настройки

Для каждого интерфейса существует **настройка DHCP-сервера**, администратор может отключить DHCP-сервер для выбранного интерфейса. Для это необходимо включить чекбокс напротив *Игнорировать интерфейс*, иначе будут видны настройки для DHCP-сервера на платформе WAF Dallas Lock. На вкладке *Основные настройки* возможно указать числовые характеристики для DHCP-сервера:

- *Старт* — параметр определяет начальный IP-адрес для раздачи DHCP-клиентам (по умолчанию 100, т.е. раздача начнется с адреса 192.168.1.100).
- *Предел* — параметр определяет, сколько всего IP-адресов можно раздать. (по умолчанию 150).
- *Время аренды* — время, через которое истекает привязка IP к MAC-адресу клиента (минимум - 2 минуты, по умолчанию — 12 часов). Можно использовать суффикс ‘m’ для указания минут, ‘h’ — часов, ‘d’ — дней.

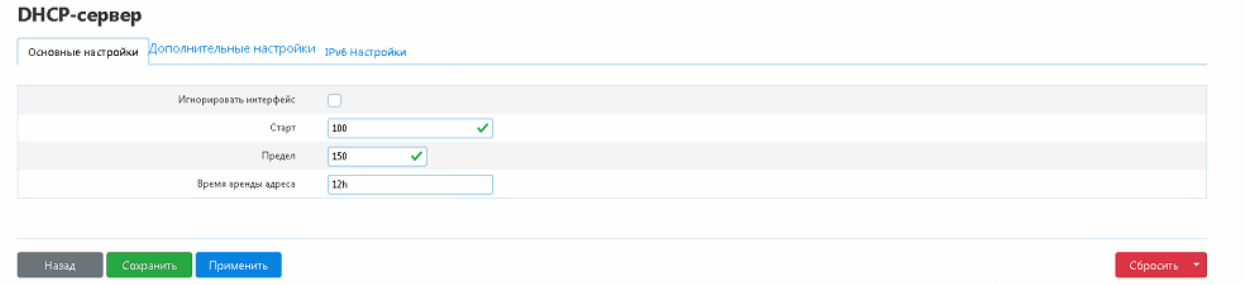


Рисунок 130. DHCP-сервер – Основные настройки

На вкладке *Дополнительные настройки* (см. Рисунок 131) можно включить протокол динамической настройки узла, позволяющий устройствам автоматически получать ip-адреса.

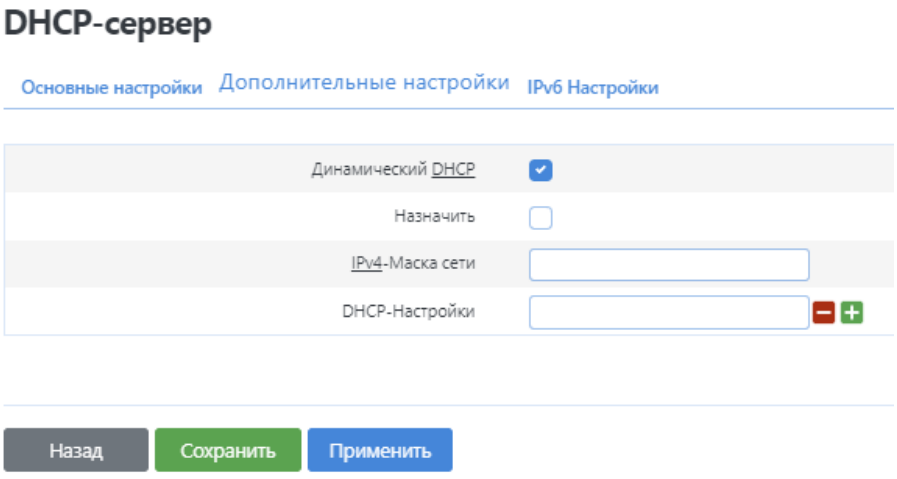


Рисунок 131. DHCP-сервер – Дополнительные настройки

На вкладке *IPv6 настройки* (см. Рисунок 132) можно настроить режим работы DHCP-сервера для сетей IPv6: режим сервера, режим передачи, гибридный режим, либо отключить вовсе. Настроить оказываемый DHCP-сервером DHCPv6-сервис: режим сервера, режим передачи, гибридный режим, либо отключить вовсе. Настроить сервис NDP-прокси: режим передачи, гибридный режим, либо отключить вовсе. А также возможно вручную указать адреса DNS-сервера, либо DNS-домена, через запятую.

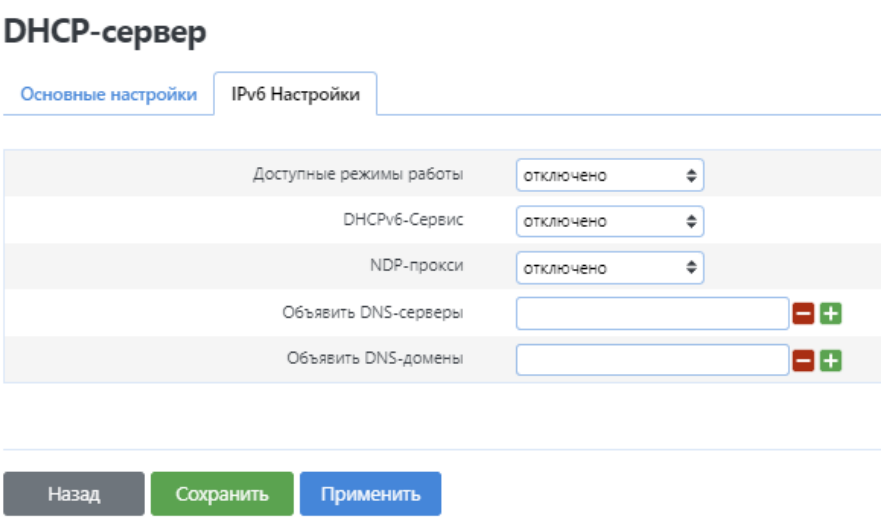


Рисунок 132. DHCP-сервер – IPv6 Настройки

6.2 DHCP и DNS

Данная страница позволяет указать настройки для DHCP-сервера и DNS-прокси для сетевых экранов NAT. На вкладке *Основные настройки* (см. Рисунок 133) можно указать основные настройки DHCP-сервера и DNS-прокси Таблицы.

На вкладке *Основные настройки* (см. Рисунок 133) содержатся следующие поля настроек:

- *Требуется домен.* При включенном чекбоксе DNS-запросы не будут перенаправляться без DNS-имени;
- *Авторизированный.* При активном чекбоксе ускоряет процесс аренды DHCP-сервер. Используется, если это единственный сервер в сети;
- *Локальный сервер.* Выдача IP-адресов происходит из файла DHCP (/etc/config/dhcp) или файла хостов (/etc/hosts);
- *Локальный домен*. В поле указывается суффикс локального домена, который будет добавлен к DHCP-именам и записи файлов и хостов (/etc/hosts);
- *Запись запросов.* При включении чекбокса позволяет записывать полученные DNS-запросы в системный журнал;
- *Перенаправление запросов DNS.* Поля содержат адреса DNS-серверов для перенаправления запросов;
- *Защита от DNS Rebinding.* При включении чекбокса система отбрасывает ответы внешней сети RFC1918, также доступны настройки:
- *Разрешить локальный хост*. При включении чекбокса разрешает исходящие ответы 127.0.0.0/8, требуемые для служб черного списка на основе DNS;
- *Белый список доменов*. Поля содержат список доменов, для которых разрешены ответы RFC1918.
- *Только локальный DNS.* При включении чекбокса система разграничивает входящий трафик от внешней сети в диапазоне 127.0.0.0/8;
- *Не использовать wildcard.* При включении чекбокса система устанавливает соединение только с определенными интерфейсами, не использующие подстановочные адреса, также доступны настройки:
  - *Интерфейс для входящих соединений.* Ограничивает прослушивание интерфейсов и замыкает их на себя (пример ввода *eth0*, *eth1*);
  - *Исключите интерфейсы.* Устанавливает запрет на прослушивание интерфейсов (пример ввода *eth0*, *eth1*).

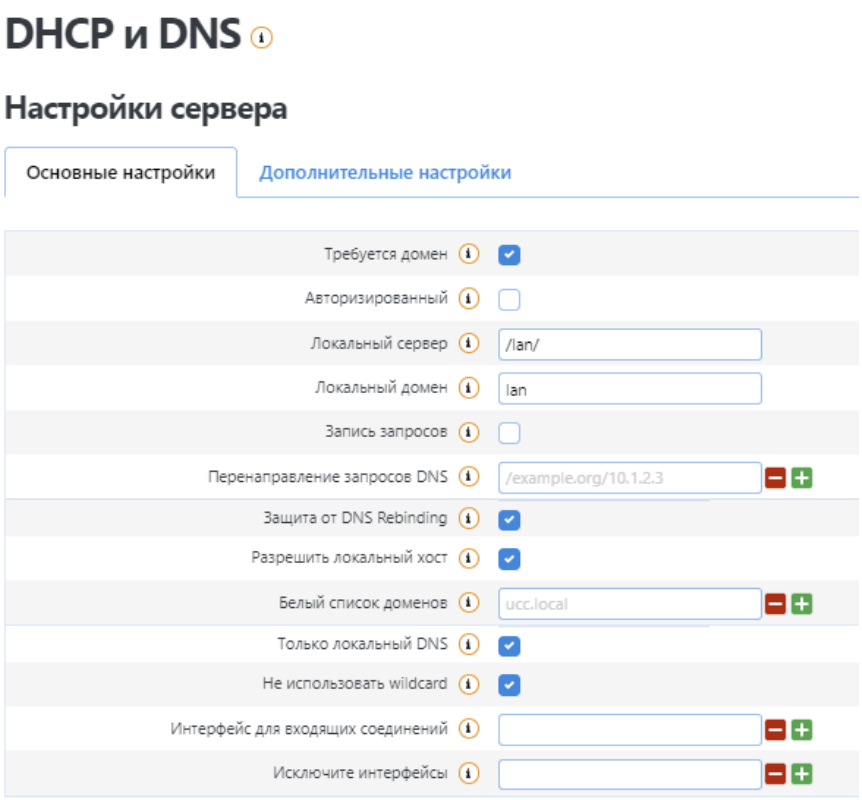


Рисунок 133. Основные настройки

Активные DHCP аренды, Активные DHCPv6 аренды (см. Рисунок 134) позволяют просматривать состояние активных арендованных адресов.
Таблица **Постоянные аренды** (см. Рисунок 134) используется для присвоения DHCP-клиентам фиксированных IP-адресов и имен. Это необходимо для статических интерфейсов, в которых обслуживаются только клиенты с присвоенными IP-адресами.

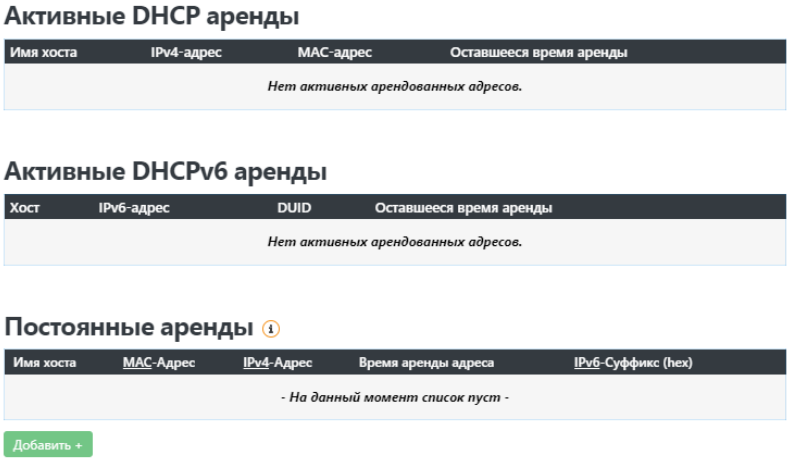


Рисунок 134. Основные настройки

Для добавления хоста в таблицу «Постоянные аренды» следует:

1. Нажать кнопку **Добавить**;
2. Ввести:

- «Имя хоста» ── название хоста (на английском языке);
- «MAC-Адрес», введенный адрес идентифицирует хост;
- «IPv4-Адрес» IP-адрес сети;
- «Время аренды адреса» время подключения (используются суффиксы «s» — для указания секунд, «m» — минут, «h» — часов, «d» — дней);

- «IPv6-Суффикс (hex)» (см. Рисунок 135).

В данном разделе настроек (см. Рисунок 135) кнопки **Удалить, Добавить**, имеют «прямой» характер работы, то есть при нажатии, действие будет происходить немедленно, в отличие от «транзакционного» характера работы других настроек в системе.

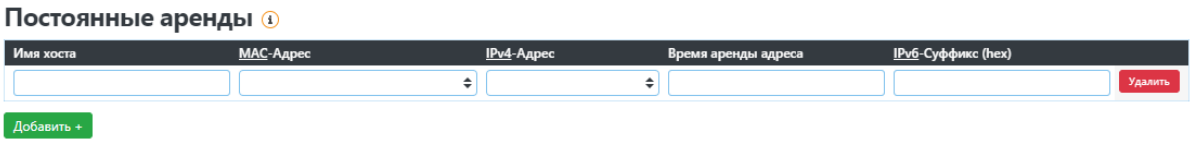


Рисунок 135. Добавление постоянной аренды

На вкладке *Дополнительные настройки* (см. Рисунок 136) содержатся следующие настройки:

- *Подавить логирование.* Устанавливает подавление логирования стандартной работы протоколов;
- *IP последовательно*. Позволяет выделять IP-адреса последовательно, начиная с наименьшего;
- *Фильтровать частные*. Позволяет системе не перенаправлять обратные DNS-запросы для локальных сетей;
- *Фильтровать бесполезные.* Не перенаправляет запросы, которые не могут быть обработаны публичными DNS-серверами;
- *Локализовывать запросы.* Локализировать имя хоста в зависимости от запрашиваемой подсети, если доступно несколько IP-адресов;
- *Расширять имена узлов.* Добавить локальный суффикс домена для имени;
- *Отключить кэш отрицательных ответов.* Позволяет не кешировать отрицательные ответы, в том числе и для несуществующих доменов;
- *Дополнительные файлы серверов.* Поле может содержать пользовательские строки или полный список внешней сети DNS-сервера;
- *Строгий порядок.* Опрос DNS-серверов будет проходить в строгом порядке;
- *Переопределение поддельного NX-домена.* Список хостов, поставляющие поддельные результаты домена NX;
- *DNS порт сервера.* Порт для входящих DNS-запросов;
- *DNS порт запроса.* Фиксированный порт для исходящих DNS-запросов;
- *Макс. кол-во аренд DHCP аренды.* Максимальное количество активных арендованных DHCP-адресов;
- *Макс. EDNS0 размер пакета.* Максимально допустимый размер UDP пакетов-EDNS.0.*;*
- *Макс. кол-во одновременных запросов.* Максимально допустимое количество одновременных DNS-запросов.

Поля настроек *Подавить логирование, IP последовательно, Фильтровать частные, Фильтровать бесполезные, Локализовывать запросы, Расширять имена узлов, Отключить кэш отрицательных ответов, Строгий порядок* требуют активного чекбокса для работоспособности.

При нажатии кнопки **Сохранить** *и* **применить** происходит запись введенных настроек в соответствующие config-файлы.

При нажатии кнопки **Сохранить** происходит сохранение введенных настроек в форме веб-интерфейса.

Нажатие кнопки **Сбросить** приводит к удалению введенных данных, которые не были сохранены (записаны в config-файлы) ранее.

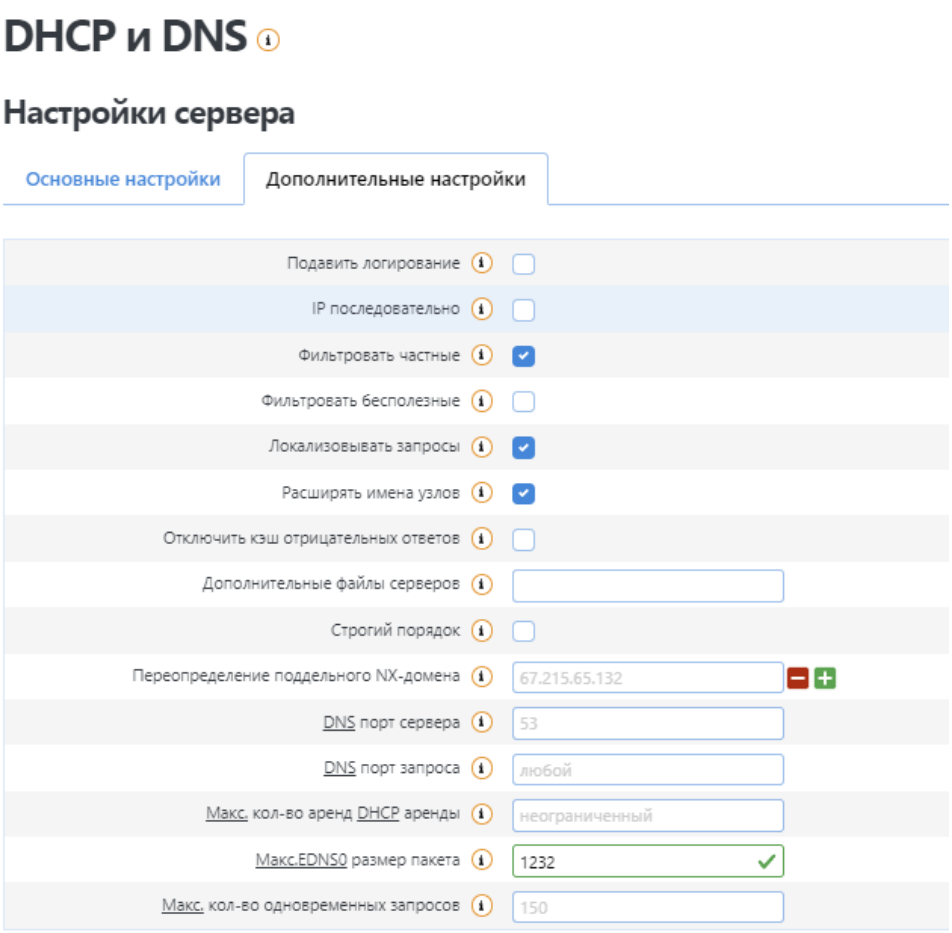


Рисунок 136. Дополнительные настройки

6.3 Имена хостов

Данная страница (см. Рисунок 137) позволяет добавить необходимые хосты в демилитаризованную зону (DMZ). Для этого необходимо указать Имя хоста и его IP-адрес, а также поставить отметку в столбце DMZ напротив добавляемого хоста.

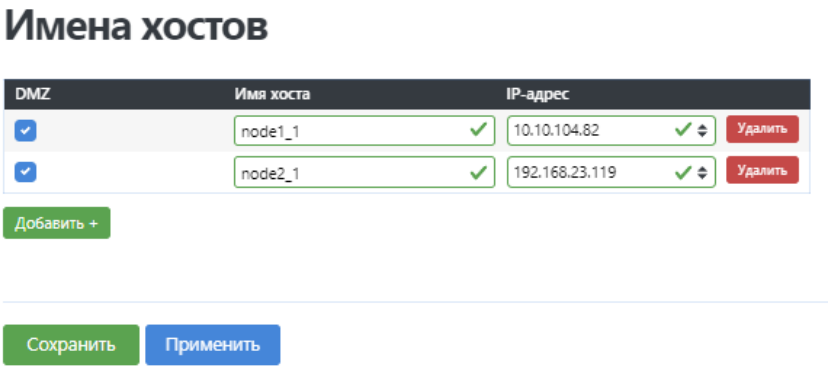


Рисунок 137. Имена хостов

6.4 Статистические маршруты

На данной странице (см. Рисунок 138) можно настроить маршрутизацию для определения, через какой интерфейс и шлюз можно достичь определенного хоста или сети.

Пункты **Статические маршруты IPv4** и **Статические маршруты IPv6** отражают имена интерфейсов, назначение (IP-адрес или сеть), маску сети (в случае IPv4), шлюз, метрику, MTU, тип маршрута.

Кнопка **Добавить** позволяет добавить новый маршрут трафика в соответствующем пункте.

Кнопка **Сохранить** позволяет применить внесенные изменения и сохранить текущую конфигурацию шлюза.

Кнопка **Применить** позволяет применить внесенные в конфигурацию изменения.

Кнопка **Сбросить** позволяет отказаться от внесенных изменений со времени последнего сохранения конфигурации.

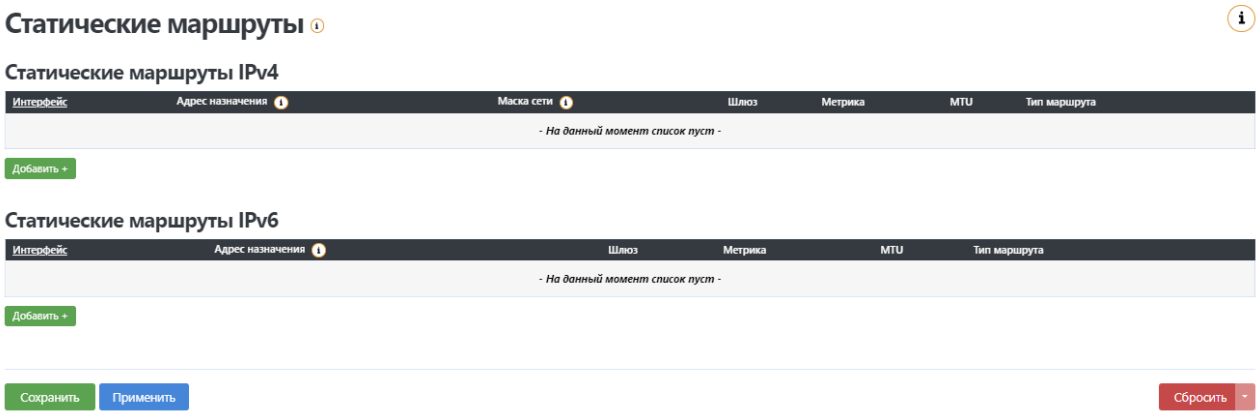


Рисунок 138. Статические маршруты

6.5 Межсетевой экран

На странице **Межсетевой экран** можно создать и настроить зоны сети для контроля трафика. Страница (см. Рисунок 139) содержит следующие вкладки:

- основные настройки;
- перенаправление портов;
- правила для трафика;
- правила аудита трафика;
- списки доступа;
- пользовательские правила.

Межсетевой экран создает зоны в сети для контроля трафика.

Кнопка **Сохранить** позволяет применить внесенные изменения и сохранить текущую конфигурацию шлюза.

Кнопка **Применить** позволяет применить внесенные в конфигурацию изменения.

Кнопка **Сбросить** позволяет отказаться от внесенных изменений со времени последнего сохранения конфигурации.

6.5.1 Основные настройки

Вкладка *Основные настройки* (см. Рисунок 139) отображает следующие настройки межсетевого экрана с выбором соответствующего действия:

- Входящий трафик (принимать/не обрабатывать/отвергать).
- Исходящий трафик (принимать/не обрабатывать/отвергать).
- Перенаправление (принимать/не обрабатывать/отвергать).

Предусмотрена опция *«Не пропускать некорректные пакеты».*

В пункте **Зоны** отображаются созданные правила МЭ. Данная таблица позволяет визуально наблюдать правила для трафика *Зона — Перенаправление*, выбранные опции для входящего/исходящего трафика, перенаправления, а также включение/отключение функций маскарадинга и ограничения MSS. Для каждого правила присутствуют отдельные кнопки **Изменить** / **Удалить**.

Кнопка **Добавить** позволяет добавить новое правило контроля трафика для МЭ.

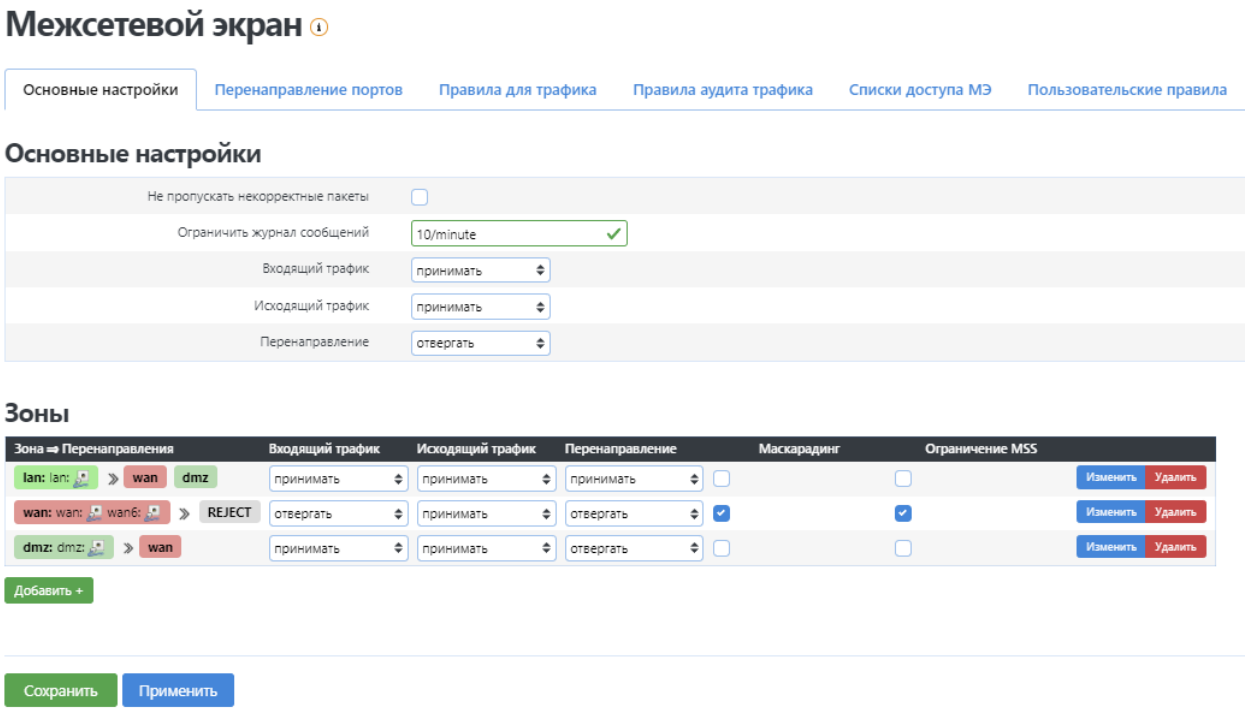


Рисунок 139. Основные настройки

6.5.2 Перенаправление портов

На вкладке можно настроить перенаправление (проброс) портов (см. Рисунок 140). Позволяет удаленным компьютерам из Интернета соединяться с компьютером или службой внутри частной локальной сети. Доступ осуществляется при помощи перенаправления трафика определенных портов с внешнего адреса на адрес выбранного компьютера в локальной сети.

Для того чтобы настроить проброс портов нужно в пункте **Новое перенаправление порта** ввести следующие значения:

- в графе *Имя* задать имя;
- в графе *Протокол* выбрать протокол, который будет использоваться для передачи данных. Выбрать необходимое значение из раскрывающегося списка;
- в графе *Внешняя зона* выбрать зону внешней сети. Выбрать необходимое значение из раскрывающегося списка;
- в графе *Внешний порт* указать порт, трафик с которого будет переадресовываться на IP-адрес, определяемый в поле Внутренний IP-адрес;
- в графе *Внутренняя зона* выбрать зону внутренней сети. Выбрать необходимое значение из раскрывающегося списка;
- в графе *Внутренний IP-адрес* указать IP-адрес устройства, находящегося в локальной сети. Необходимо выбрать устройство, подключенное к локальной сети в данный момент. Для этого в раскрывающемся списке выбрать соответствующий IP-адрес (при этом поле заполнится автоматически), либо задать его вручную, выбрав в раскрывающемся списке *«Пользовательский»;*
- в графе *Внутренний порт* указать порт, на который будет переадресовываться трафик с порта, задаваемого в поле *Внешний порт.*

После задания необходимых значений нужно нажать кнопку **Добавить**. После этого в графе *Перенаправление портов* появится правило перенаправления. В списке можно редактировать правила, а также включать/отключать и сортировать их.

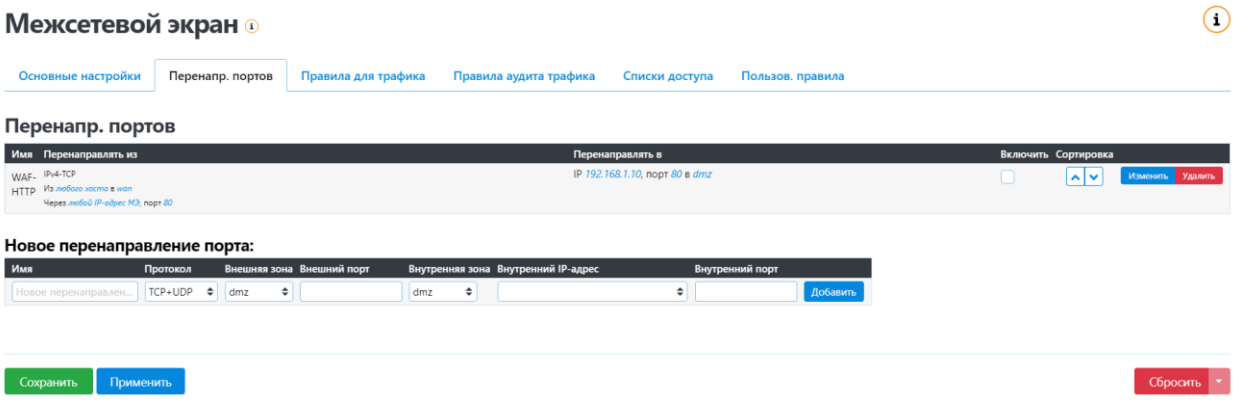


Рисунок 140. Перенаправление портов

6.5.3 Правила для трафика

На данной вкладке можно настроить правила для трафика (см. Рисунок 141), которые определяют политику прохождения пакетов между разными зонами, например, запрет трафика между некоторыми хостами или открытие WAN-портов маршрутизатора.

Пункт **Правила для трафика** содержит список созданных правил. Данная таблица позволяет визуально наблюдать правила аудита, а также сортировать и включать/отключать их. Для каждого правила присутствуют отдельные кнопки **Изменить**/**Удалить**.

Пункт **Открыть порты на МЭ** позволяет добавить порт, который необходимо открыть на МЭ. Для этого необходимо добавить имя нового правила для входящего трафика, указать протокол и внешний порт, далее нажать кнопку **Добавить**.

Пункт **Новое правило перенаправления** позволяет создавать новые правила перенаправления трафика, а также редактировать существующие. При создании нового правила перенаправления указывается его имя, зоны источника и назначения. Кнопка **Добавить и редактировать…** позволяет сохранить новое правило или редактировать уже имеющееся.

Пункт **Правила для SNAT** отображает список созданных NAT-источников. Таблица позволяет визуально наблюдать список источников, а также сортировать и включать/отключать их.

Пункт **Новое правило для SNAT** позволяет задать новый или редактировать SNAT. SNAT — это особая форма маскарадинга (masquerading), позволяющая осуществлять детальный контроль над IP-адресом источника для исходящего трафика, например, перенаправление нескольких WAN-адресов во внутреннюю подсеть.

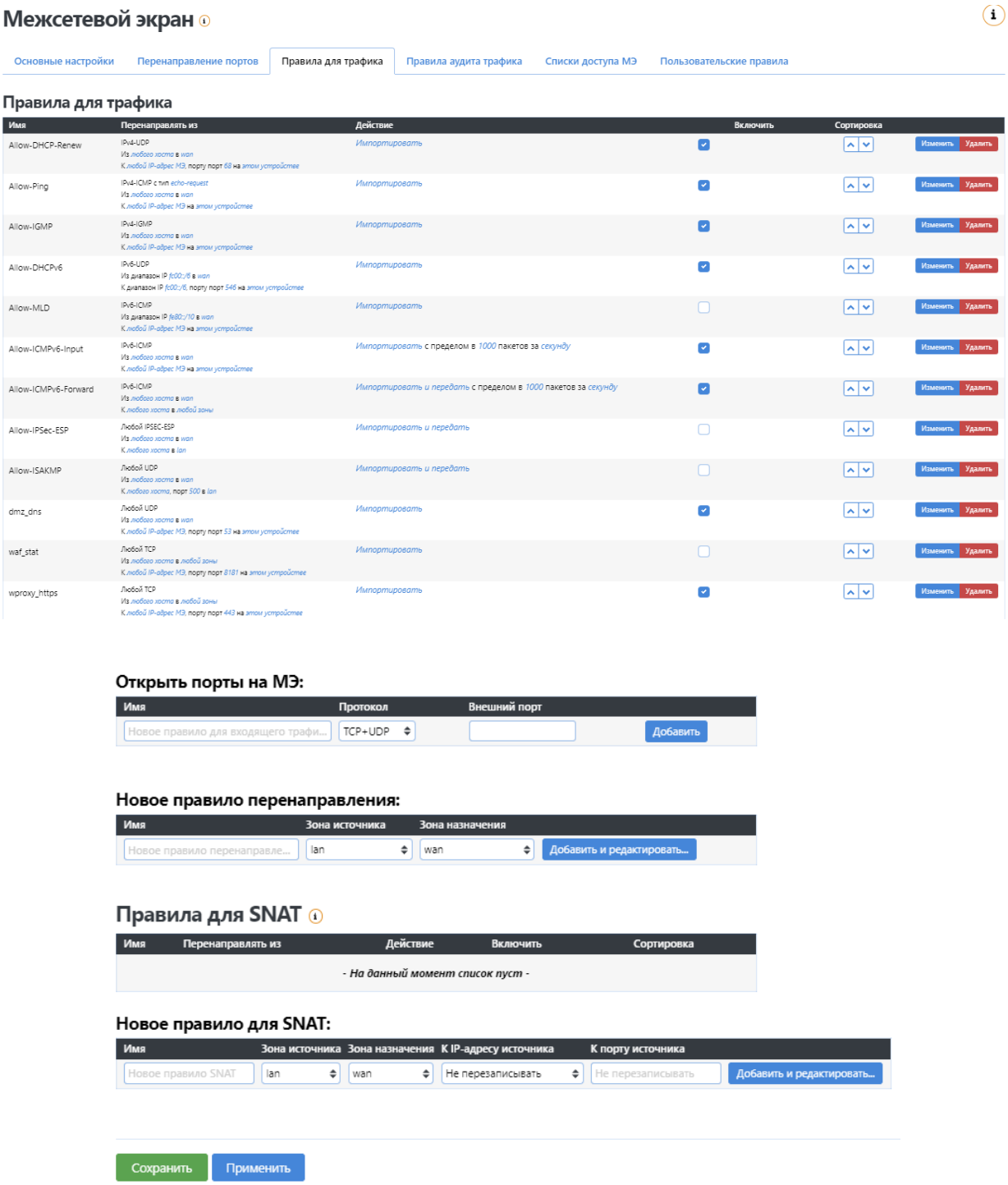


Рисунок 141. Правила для трафика

6.5.4 Правила аудита трафика

На данной вкладке можно настроить правила аудита трафика (см. Рисунок 142), которые определяют политику логирования проходящих пакетов между разными зонами, например, трафик с определенного хоста, перенаправляемый к другому хосту.

В пункте **Правила аудита трафика** отображаются созданные правила аудита. Данная таблица позволяет визуально наблюдать правила аудита, а также сортировать и включать/отключать их.

При создании нового правила аудита в пункте **Новое правило аудита** указывается его имя, зоны источника и назначения, а также префикс. Кнопка **Добавить и редактировать…** позволяет сохранить новое правило или редактировать уже имеющееся.

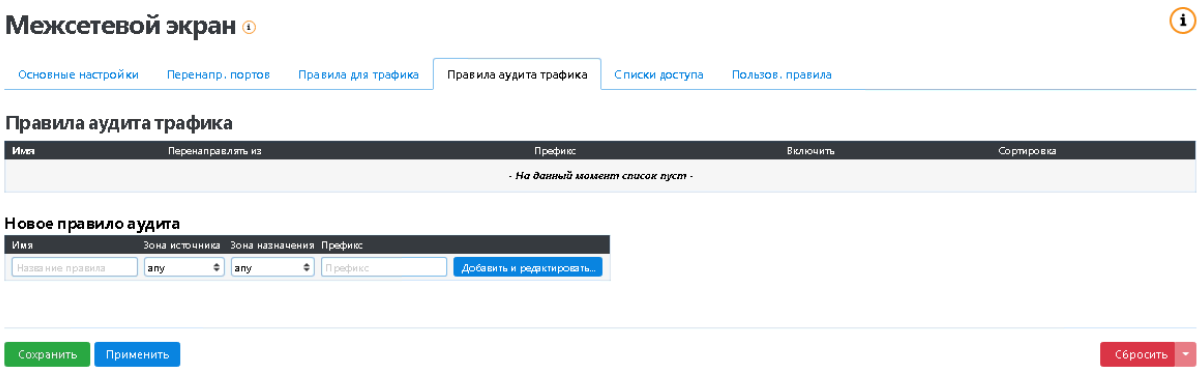


Рисунок 142. Правила аудита трафика

6.5.5 Списки доступа МЭ

На данной вкладке настраиваются списки доступа (см. Рисунок 143) для блокировки сетей и хостов, являющихся источниками угроз защищаемым ресурсам, а также для указания сетей и хостов, не подлежащих блокировке. **WAF Dallas Lock** позволяет добавлять и блокировать адреса IPv4 и IPv6.

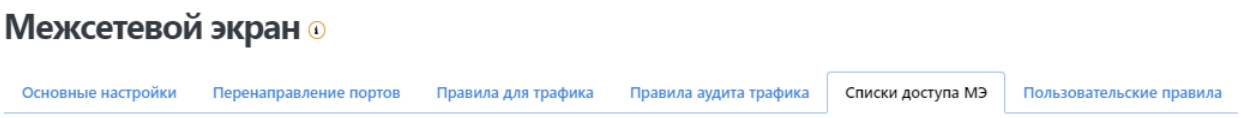


Рисунок 143. Списки доступа МЭ

В таблицах **Разрешенные узлы, Разрешенные сети, Разрешенные IPv6 узлы, Разрешенные IPv6 сети, Запрещенные узлы, Запрещенные сети, Запрещенные IPv6 узлы, Запрещенные IPv6 сети** отображается информация о добавленных пользователем соединениях. В столбцах *Хост* отображаются подключенные IP-адреса. В столбцах *Таймаут* — оставшееся время подключения IP-адресов к системе **WAF Dallas Lock** (см. Рисунок 144).

В данном разделе настроек (см. Рисунок 144) кнопки **Удалить, Постоянная аренда**, имеют «прямой» характер работы, то есть при нажатии, действие будет происходить немедленно, в отличие от «транзакционного» характера работы других настроек в системе.

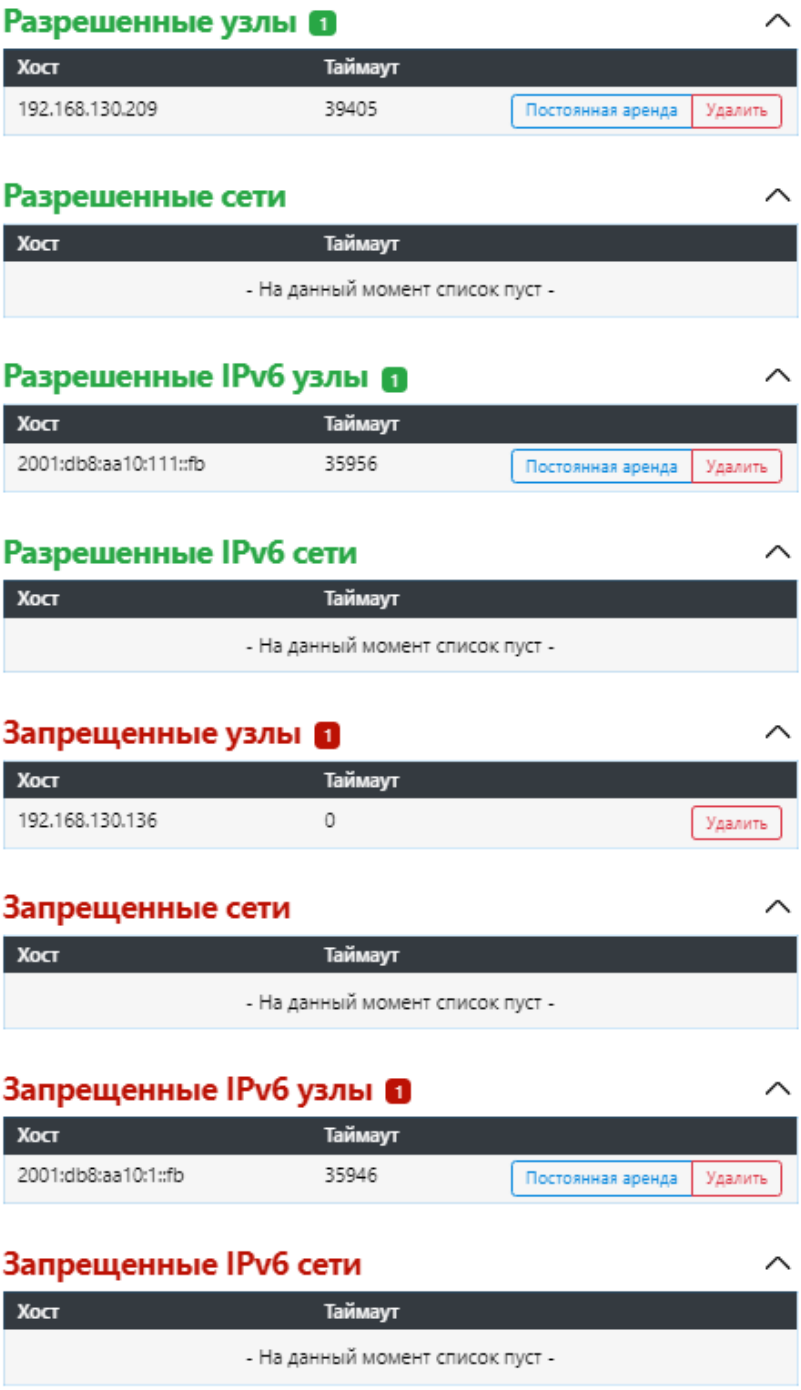


Рисунок 144. Списки доступа МЭ

Блок управляющих кнопок (см. Рисунок 145):

- **Фильтр**. Сортирует значения в таблицах исходя из введенных данных в поле *Фильтр*;
- **Добавить**. По кнопке появляется всплывающие окно для добавления нового соединения;
- **Скачать**. Сохраняет все настройки в файл в формате *rules*.

В строке таймаут задается время в секундах, которое будет устанавливаться по умолчанию при добавлении в список разрешенных/запрещенных сетей/хостов (значение 0 - постоянная аренда (подключение)) (см. Рисунок 145).

Новое значение таймаута вступит в силу только после перезагрузки **WAF Dallas Lock.**

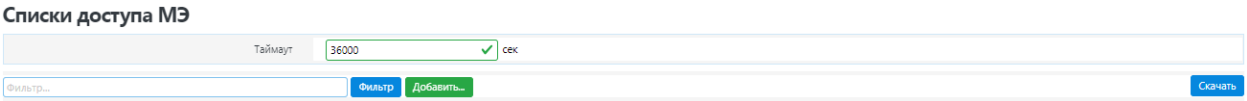


Рисунок 145. Функционал кнопок

Для добавления нового соединения в таблицы разрешенные/запрещенные узлы/хосты требуется выполнить следующие действия:

1. Нажать кнопку **Добавить**;
2. В сплывающем окне *Добавление нового IP* (см. Рисунок 146) установить переключатель на значение *Список запрещенных* или *Список разрешенных*;
3. Ввести в поле *IP* IP адрес сети/хоста и в поле *Таймаут* время подключения;
4. Нажать кнопку **Добавить** на форме *Добавление нового IP (*кнопка **Закрыть** – отменяет действие, изменения не сохраняются).

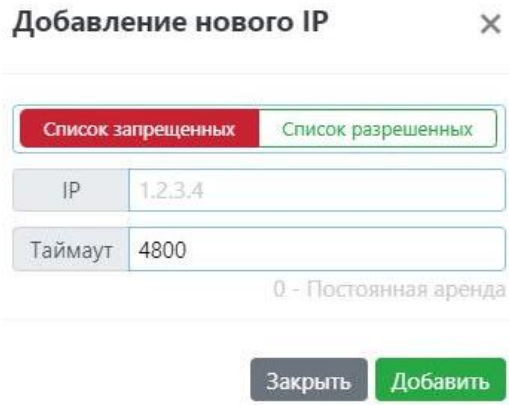
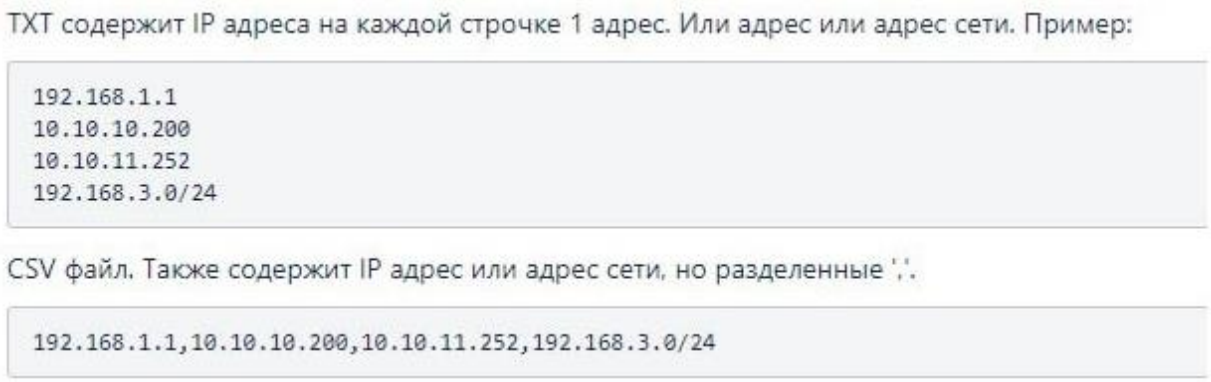


Рисунок 146. Добавление нового IP

В **Списках доступа МЭ** реализована возможность загружать пользовательские списки и взаимодействовать с ними (см. Рисунок 148). Загружать списки возможно в **Список запрещенных узлов** и **в Список разрешенных узлов.**
Для взаимодействия со списком/списками необходимо включить чекбокс напротив списка/списков и нажать управляющую кнопку:

- **Включить/Выключить**. Кнопки активируют/деактивируют работу списка/списков;
- **Загрузить**. Позволяет пользователю загрузить свой список адресов в систему для дальнейшей работы с ними. Поддерживаются расширения файлов: *csv*, *txt* (см. Рисунок 147);



- **Рисунок 147. Пример файла с IP-адресами**

- **Обновить**. Кнопка отвечает за обновление списков в системе. Избавляет от необходимости вручную удалять уже имеющийся список и загружать его новую версию;
- **Обновление по расписанию**. Кнопка позволяет пользователю обновлять внесенные списки через заданный временной интервал;
- **Удалить**. Кнопка удаляет выбранный список/списки.

WAF-IP-Blacklist.lst – Список заблокированных IP-адресов, который обновляется на сайте нашей компании (Список по умолчанию).

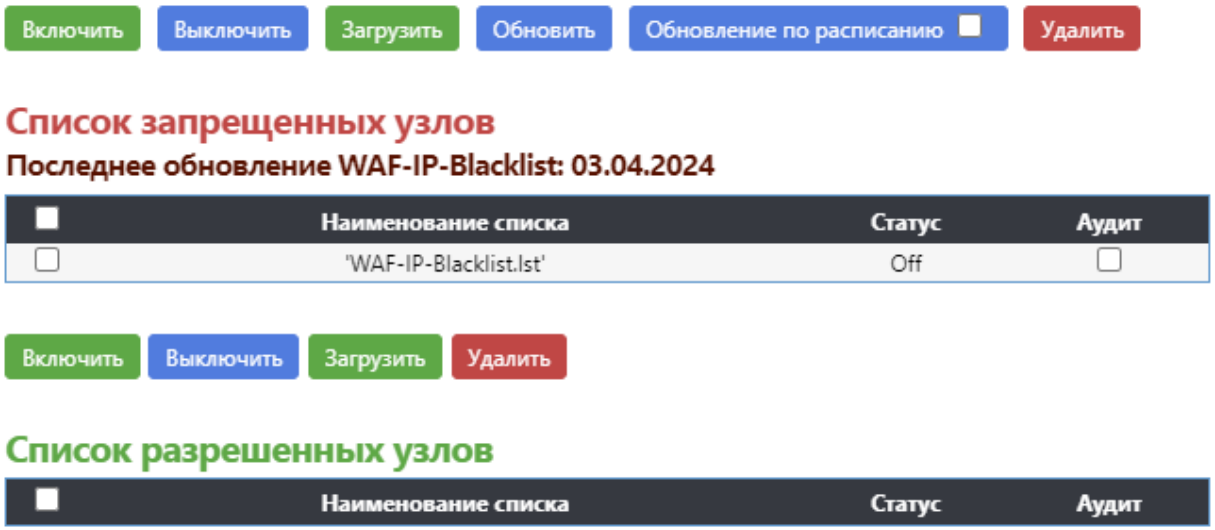


Рисунок 148. Загрузка списков

Для сохранения и применения внесенных изменений необходимо нажать кнопку **Применить**. Кнопка **Сбросить** отвечает за сброс данных фильтра, выставленного времени в Таймаут, активных чекбоксов и удаленных списков до того, как нажали кнопку **Применить**.

6.5.6 Пользовательские правила

На данной вкладке можно настроить пользовательские правила (см. Рисунок 149). Эти правила позволяют выполнять произвольные команды *iptables*, которые не охвачены рамками межсетевого экрана. Команды выполняются после каждой перезагрузки межсетевого экрана, сразу после загрузки набора правил по умолчанию.

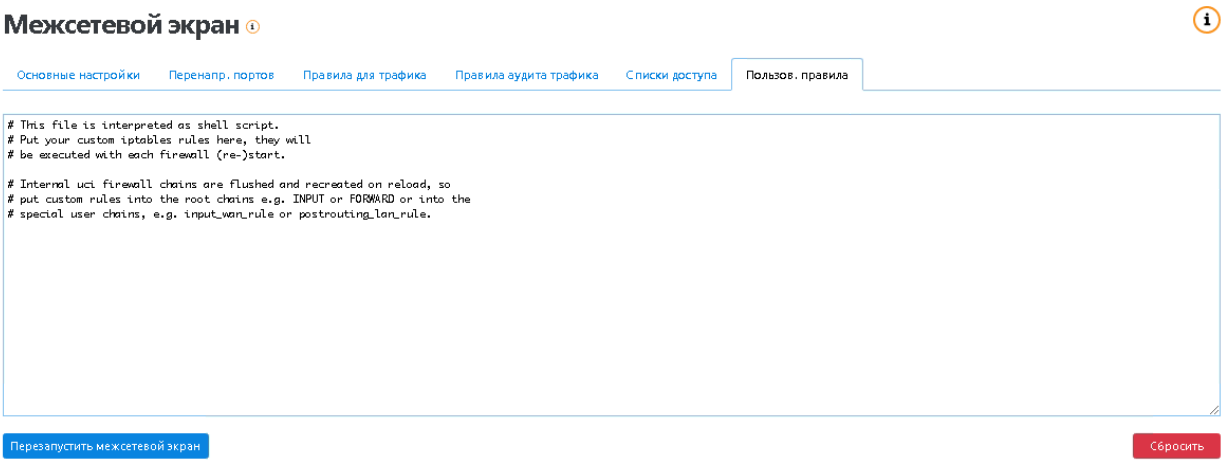


Рисунок 149. Пользовательские правила

6.6 Качество обслуживания (QoS)

На данной странице (см. Рисунок 150) можно настроить правила предоставления различным классам трафика различных приоритетов в обслуживании по адресам, портам и сервисам. Правила классификации так же могут быть настроены индивидуально для каждого интерфейса.

Интерфейсы. В данном разделе вы можете настроить приоритет интерфейса (wan, wan6, lan, dmz) и задать для них индивидуальные настройки. Для этого необходимо в раскрывающемся меню выбрать интерфейс и нажать кнопку **добавить**.

- *Подсчитывать возможное превышение трафика.*
- *Резервировать канал управления*. Резервирование канала 5% от общей полосы пропускания для гарантированного доступа к веб-интерфейсу WAF Dallas Lock.

- *Скорость получения и передачи данных***.** Настройка максимальной ширины канала для выбранного интерфейса.

Правила классификации. В данном разделе вы можете настроить приоритет по IP-адресам и для назначения результирующего решения о пропуске трафика, указав в настройках хост источника и хост назначения, протокол, порты и максимальную пропускную способность.

- *Приоритетный*. Данное назначение имеет максимальный приоритет над остальными.
- *Экспресс***.** Данное назначение предназначено для интерактивных приложений, которым требуется высокая пропускная способность.
- *Обычный*. Данное назначение используется для остальных сервисов, которые не классифицируются отдельно.
- *Большой объем***.** Выделяется оставшаяся полоса пропускания. Если канал занят привилегирующими назначениями, этому классу будет выделен только 1% от общего установленного лимита. Используйте это назначение для P2P и таких сервисов загрузки, как FTP.

При задании политики приоритизации трафика, в ситуациях когда полоса пропускания, отведенная определенному типу трафика при постоянном наличии данного трафика в сети ниже условных 10%, может наблюдаться замедление работы **WAF Dallas Lock**, обусловленное высокой нагрузкой на ЦПУ для обеспечения данной политики.
При сокращении резервированной полосы пропускания для доступа к веб-интерфейсу ниже 5 мегабит возможны ситуации «данные не получены» для работы информационной панели.

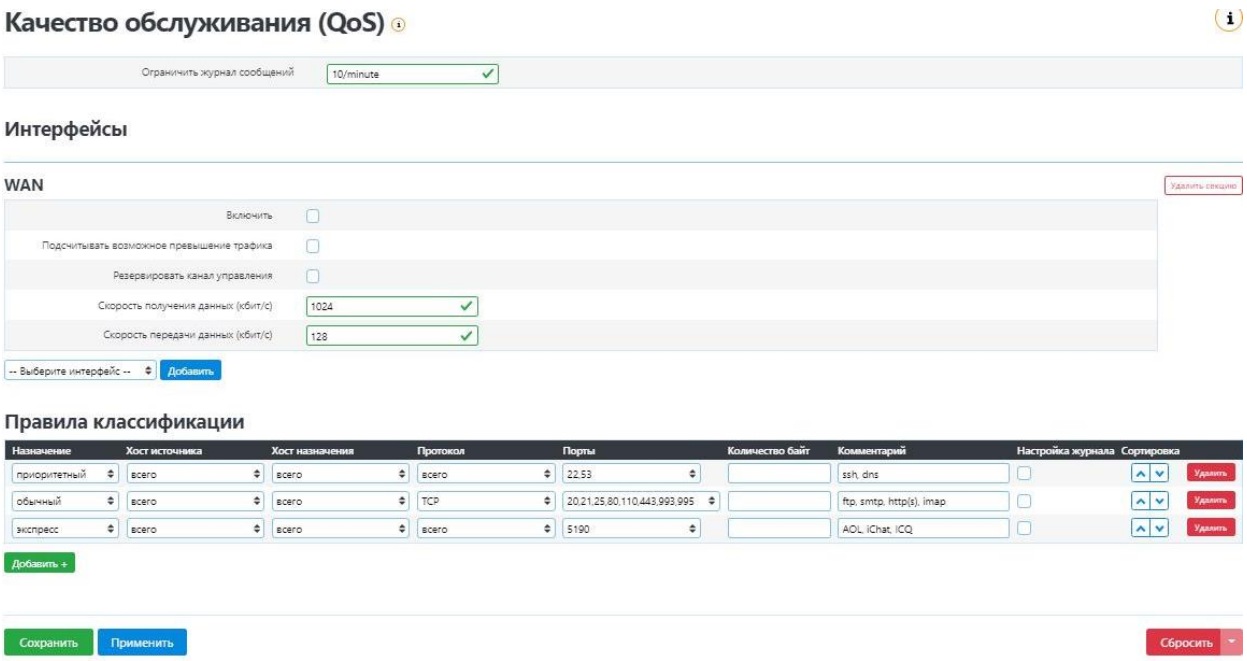


Рисунок 150. Качество обслуживания (QoS)

6.7 Диагностика

На данной странице (см. Рисунок 151) можно произвести диагностику работы системы — проверить *ping* или выполнить трассировку маршрута и таким образом проверить доступность сервера, а также выполнить DNS-запрос.

Результаты выполнения той или иной команды предоставляются ниже на той же странице.

Рисунок 151. Диагностика

Изменения

В таблице приведены сведения о последних изменениях данного документа, включая версию, дату, автора и краткое описание изменений.

Версия	Дата	Автор	Изменения