

УТВЕРЖДЕН
ПФНА.26.20.40.143.001 РЭ-ЛУ
(взамен ПФНА.501540.001 РЭ)

ШЛЮЗ БЕЗОПАСНОСТИ

WAF Dallas Lock

(версия 2.16.31.2)



Руководство по эксплуатации

ПФНА.26.20.40.143.001 РЭ
(взамен ПФНА.501540.001 РЭ)

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.ru.

СОДЕРЖАНИЕ

АННОТАЦИЯ	2
ВВЕДЕНИЕ	6
ТЕРМИНЫ И СОКРАЩЕНИЯ.....	7
1 ОБЩИЕ СВЕДЕНИЯ	8
1.1 Назначение и возможности	8
1.2 Принципы функционирования	8
1.3 Роли пользователей	9
1.4 Структура и составные модули	9
2 ПЕРВИЧНАЯ НАСТРОЙКА WAF DALLAS LOCK	14
2.1 Требование к техническому обеспечению	14
2.2 Требование к программному обеспечению	14
2.3 Требование к среде виртуализации	14
2.4 Процедура установки WAF Dallas Lock	14
2.5 Доступ к средствам администрирования	18
2.6 Настройка перенаправления DNS-запросов	19
2.7 Лицензирование продукта	20
2.8 Добавление защищаемого ресурса.....	20
3 ИНФОРМАЦИОННАЯ ПАНЕЛЬ	24
3.1 Виджет «Атакуемые ресурсы»	24
3.2 Виджет «Аппаратное обеспечение».....	24
3.3 Виджет «Все зафиксированные атаки»	25
3.4 Виджет «Источники атак».....	25
3.5 Виджет «Атаки, зафиксированные на ресурсы».....	26
3.6 Виджет «Источники атак, зафиксированные на ресурсы»	27
3.7 Виджет «Уровни тревоги атак»	27
3.8 Виджет «Уровни тревоги атак, зафиксированные на ресурсы»	28
3.9 Блок «Список инцидентов»	29
3.10 Виджет «Трафик в реальном времени»	30
3.11 Виджет «Запросы в реальном времени».....	30
4 ЖУРНАЛЫ И СТАТИСТИКА.....	32
4.1 Журналы аудита	32
4.1.1 Доступ к журналам аудита	32
4.1.2 Содержание журналов аудита	33
4.1.3 События журналов аудита	34
4.1.4 Сортировка записей аудита	35
4.1.5 Выгрузка журналов аудита.....	36
4.2 Журнал ядра	37
4.3 Журналы аварийного режима	37
4.4 Сеть	38
4.4.1 Сетевая статистика	38
4.4.2 Состояние межсетевого экрана	38

4.4.3	Маршруты	39
4.5	Графики в реальном времени.....	40
4.6	Процессы.....	41
4.7	Сведения о системе	42
5	НАСТРОЙКА WAF DALLAS LOCK	45
5.1	Настройки WAF.....	45
5.1.1	Инспекция WAF	45
5.1.2	Ресурсы WAF	48
5.1.3	Настройка кластеризации	58
5.1.4	Фильтр содержимого.....	60
5.1.5	Настройка инспекции защищаемого узла.	69
5.2	Настройки UTM	69
5.2.1	Инспекция HTTPS/HTTP	70
5.2.2	Фильтр содержимого.....	70
5.3	Настройки модуля ЕЦУ	81
5.3.1	Единый центр управления Dallas Lock	81
5.3.2	Регистрация WAF Dallas Lock в домене безопасности ЕЦУ	82
5.4	Общие настройки	83
5.4.1	Система	83
5.4.2	Настройки интерфейса управления WAF Dallas Lock.....	85
5.4.3	Параметры аудитора	93
5.4.5	Фильтр содержимого.....	97
5.4.6	Управление службами	100
5.4.7	Запланированные задания	101
5.4.8	Резервное копирование и перепрошивка.....	101
5.5	Настройка пользователей	103
5.6	Настройка сервисов	105
5.6.1	Настройка почтовых уведомлений.....	105
5.6.2	Настройка сторожевого таймера	105
5.7	Управление сертификатами	106
5.7.1	Серверные сертификаты	106
5.7.2	Сертификаты УЦ	107
5.7.3	Клиентские сертификаты.....	108
5.8	Защита от DoS/DDoS атак.....	109
5.8.1	Прикладной уровень (WAF)	109
5.8.2	Транспортный уровень	110
5.9	Настройка аварийного режима	112
5.9.1	Список сбоев	112
5.9.2	Возвращение к нормальному режиму работы	113
5.10	GEO IP фильтр	113
6	СЕТЬ	115
6.1	Интерфейсы.....	115

6.2 DHCP и DNS.....	122
6.3 Имена хостов.....	125
6.4 Статистические маршруты	126
6.5 Межсетевой экран.....	126
6.5.1 Основные настройки	126
6.5.2 Перенаправление портов.....	127
6.5.3 Правила для трафика	129
6.5.4 Правила аудита трафика.....	131
6.5.5 Списки доступа МЭ.....	133
6.5.6 Пользовательские правила.....	135
6.6 Удаленный доступ.....	136
6.6.1 Основные настройки	136
6.6.2 Реквизиты для входа.....	137
6.6.3 Создание удаленного подключения	137
6.7 Качество обслуживания (QoS)	141
6.8 Диагностика	142

ВВЕДЕНИЕ

Данное руководство предназначено для администраторов **Шлюза безопасности Web Application Firewall Dallas Lock** (далее по тексту — **WAF Dallas Lock**), осуществляющих первоначальную настройку межсетевого экрана 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 или в архиве поставки изделия в виде ISO-образа с первоначальной конфигурацией, который инсталлируется на физическое устройство или виртуальную машину. Виртуальные машины **WAF Dallas Lock** разворачиваются в выделенной виртуальной инфраструктуре клиента в средах VMware ESXi, VMware Workstation, 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
DL	Dallas Lock
DMZ	Demilitarized Zone, демилитаризованная зона
LAN	Local Area Network, локальная вычислительная сеть
UTM	Unified threat management, универсальное решение, обеспечивающее комплексную защиту от сетевых угроз
VRRP	Virtual Router Redundancy Protocol, сетевой протокол, предназначенный для увеличения доступности ресурсов, защищаемых WAF DL
WAN	Wide Area Network, глобальная компьютерная сеть
VLAN	Virtual Local Area Network, виртуальная локальная сеть
WAF	Web Application Firewall, межсетевой экран для защиты веб-сервера

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение и возможности

WAF Dallas Lock — межсетевой экран прикладного уровня, реализующий функции контроля и фильтрации информационных потоков для защиты логических границ сети и веб-серверов, расположенных в демилитаризованной зоне, обеспечивающий обнаружение и блокирование угроз безопасности информации.

WAF Dallas Lock включает в себя два отдельно лицензируемых функциональных модуля:

- WAF (Web Application Firewall) — межсетевой экран уровня веб-сервера;
- UTM (Unified Threat Management) — межсетевой экран уровня логических границ сети и система обнаружения вторжений уровня сети.

WAF Dallas Lock обладает следующими основными возможностями:

- централизованный мониторинг и управление защитой нескольких веб-приложений из единой консоли;
- 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;
- защита от DoS/DDoS атак на прикладном и транспортном уровнях модели OSI;
- фильтрация сетевого трафика по заданным правилам с возможностью настройки правил и политик фильтрации;
- защита файлов cookie от несанкционированного раскрытия и нарушения целостности;
- ограничение доступа к защищаемым ресурсам из определенных стран по геолокации на основе IP-адреса;
- использование нейронных сетей для анализа входящего трафика и обнаружения вторжений;
- анализ поведения пользователей, обнаружение аномальной активности и блокировка трафика на основании графов связей и переходов на защищаемом ресурсе;
- создание удаленного подключения к автоматизированным рабочим местам в локальной вычислительной сети (LAN) из глобальной сети Интернет (WAN);
- поддержка технологии виртуальных локальных сетей (VLAN);
- интеграция с **Единым центром управления Dallas Lock**;
- интеграция в SIEM-систему по протоколу syslog в формате leaf;
- возможность кластеризации нескольких серверов с **WAF Dallas Lock**.

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).

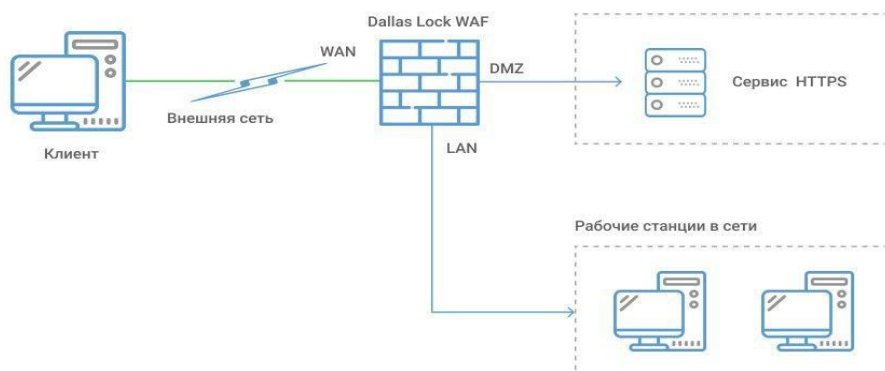


Рисунок 1. Типовая схема использования WAF Dallas Lock

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 экранирования. Межсетевое экранирование, обнаружение вторжений и защита веб-серверов реализуются заданием и своевременным обновлением администратором правил фильтрации и баз разрешающих правил.

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-интерфейса, 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 разделах [5.4.2 Настройки интерфейса управления WAF Dallas Lock](#) и [5.5 Настройка пользователей](#).

Аудитор (auditor) — пользователь, наделенный правами на просмотр параметров и журналов системы защиты. Подробнее об этой роли в разделе [5.4.3 Параметры аудитора](#).

Внутренний пользователь (subadmin) — пользователь, имеющий доступ только к консольной оболочке WAF. Может выполнять конкретные команды, описанные в разделе [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 пользователя и 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 **ЕЦУ** (иконка не отображается, если не зарегистрирован в домене безопасности);
 - переключение между светлой и темной темой графического интерфейса **WAF Dallas Lock**.

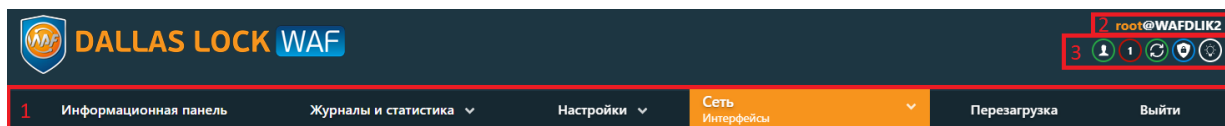


Рисунок 2. Меню управления WAF Dallas Lock

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** или **Добавить 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 уровня веб-сервера (тип Г), а также инструментарий для поиска и сортировки этих данных.
- **Трафик в реальном времени.** График входящего и исходящего трафика реализован по защищаемым ресурсам в реальном времени.
- **Запросы в реальном времени.** График запросов в секунду в реальном времени.

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

Включает в себя:

- **Журналы аудита.** Страница содержит следующие журналы (вкладки):
 - *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 веб-сервера; анализе поведения пользователей нейронными сетями; сравнении действий пользователей с параметрами графа связей.
 - *COB.* Журнал *COB* 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 логических границ 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 и параметров автозапуска служб **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 события режима усиленной защиты от DoS/DDoS атак.
- *Прокси.* Журнал *Прокси* содержит события по регистрации HTTP-запросов к веб-приложению.



Возможна выгрузка выбранного журнала путем нажатия кнопки **Сохранить**. Факт выгрузки журнала фиксируется в системном журнале. Кнопки **На архивный** и **На текущий** позволяют перейти к просмотру архивных и текущих журналов соответственно (по умолчанию кнопки не активны, для активации кнопок необходимо загрузить архивный журнал, подробнее в разделе [5.4.3 Параметры аудитора](#)).

- **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 для сетевых интерфейсов (зоны LAN, WAN и DMZ) **WAF Dallas Lock**.
 - *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 **Завершить принудительно**.
- **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 шлюза безопасности **WAF Dallas Lock**. Включает в себя:

- **WAF.** Содержит параметры межсетевого экрана уровня веб-сервера.
 - *Инспекция WAF* — содержит две уточняющие вкладки: *Основные настройки*, *Клиенты*. Вкладка *Основные настройки* позволяет настроить общие параметры работы процедуры инспекции. Вкладка *Клиенты* позволяет настроить аутентификацию клиентов с использованием центров сертификации.
 - *Ресурсы WAF* — содержит две уточняющие вкладки: *Защищаемые серверы*, *Защищаемые ресурсы*. Вкладка *Защищаемые серверы* позволяет управлять защищаемыми серверами. Вкладка *Защищаемые ресурсы* позволяет добавить новые объекты защиты (домены для инспекции), а также выбрать профиль

- приложения, развернутого на этом объекте, указать требуемую политику контента для развернутого приложения и настроить анализ поведения пользователей на основании графа связей.
- *Настройка кластеризации* — функциональная возможность работы в режиме отказоустойчивого кластера по схеме Active-Passive и миграции конфигурационных настроек между несколькими машинами.
 - *Фильтр содержимого* — позволяет 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.
 - **UTM.** Содержит параметры межсетевого экрана уровня логических границ сети и системы обнаружения вторжений уровня сети.
 - *Инспекция HTTPS/HTTP* — позволяет настроить параметры инспекции HTTPS/HTTP трафика.
 - *Фильтр содержимого* — позволяет настроить основные параметры UTM, COB и МЭ уровня логических границ сети, настроить параметры защиты от несигнатурных угроз и обновить БРП.
 - **Настройки модуля ЕЦУ.** Обеспечивает взаимодействие между шлюзом безопасности WAF Dallas Lock и Единым центром управления Dallas Lock (ЕЦУ).
 - **Общие.** Позволяет настроить общие параметры шлюза безопасности WAF Dallas Lock.
 - *Система* — позволяет задать параметры устройства, такие как дата и время, имя хоста, часовой пояс, настроить синхронизацию времени и управлять файлами лицензий.
 - *Настройки интерфейса управления WAF Dallas Lock* — позволяет задать пароль администратора, параметры управления через веб-интерфейс и подключения к консоли WAF Dallas Lock по протоколу SSH.
 - *Параметры аудитора* — позволяет настроить параметры аудита, архивировать журналы и задать пороговые значения для реакции WAF Dallas Lock на инциденты безопасности.
 - *Фильтр содержимого* — позволяет настроить количество обслуживающих процессов и переменных фильтра содержимого.
 - *Управление службами* — позволяет включить или отключить установленные скрипты инициализации.
 - *Запланированные задания* — позволяет создать и применить задание для планировщика задач.
 - *Резервное копирование и восстановление* — позволяет создать архив конфигурационных настроек, восстановить конфигурацию, обновить прошивку WAF Dallas Lock и осуществить сброс к заводским настройкам.
 - **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.** В разделе реализована функциональная возможность управления сервисами WAF Dallas Lock. Страницы раздела позволяют настроить следующие параметры:
 - *Почтовые уведомления* — позволяет задать параметры почтового сервера для уведомления администратора о событиях информационной безопасности по электронной почте.
 - *Сторожевой таймер* — позволяет настроить работу сторожевого таймера в режиме «Перезагрузка при потере интернет соединения» или «Периодическая перезагрузка».
 - **Управление сертификатами.** Представляет собой службу создания, обновления и замены цифровых сертификатов.
 - **Защита от DoS/DDoS.** На странице реализована функциональная возможность настройки параметров защиты от DoS/DDoS атак на прикладном и транспортном уровнях сетевой модели OSI.
 - **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.** На странице реализована 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.
- **Удаленный доступ.** На данной странице возможно настроить параметры удаленного доступа к локальной вычислительной сети, защищенной **WAF Dallas Lock**, а также управлять учетными данными для такого подключения.
- **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 должен составлять не менее 32 Гб;
- объем памяти накопителя для хранения журналов аудита должен составлять не менее 128 Гб;
- количество сетевых интерфейсов типа RJ45 или SPF+, поддерживающих скорость передачи данных не менее 1 Гб/с, должно составлять не менее трех (LAN, WAN, DMZ). При этом типы интерфейсов зон DMZ и LAN должны совпадать с типом интерфейса зоны WAN и обеспечивать не меньшую скорость передачи данных;
- должно обеспечиваться наличие режима совместимости (MBR) в BIOS.



Для работы отдельно лицензируемых модулей достаточно использовать два интерфейса: для UTM — LAN и WAN, а для WAF — DMZ и WAN. Для корректного функционирования модуля WAF необходимо настроить доступ к управлению межсетевым экраном, поскольку по умолчанию этот доступ возможен только с интерфейса LAN (см. [5.4.2.3 Управление доступом к межсетевому экрану](#)).

2.2 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 Browser 14 и выше.

2.3 Требование к среде виртуализации

WAF Dallas Lock может использоваться в виртуальной среде. Виртуальные машины WAF Dallas Lock разворачиваются в выделенной виртуальной инфраструктуре клиента в средах:

- VMware ESXi;
- VMware Workstation;
- Hyper-V;
- VirtualBox.

2.4 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.

Чтобы загрузиться в режиме UEFI, необходимо выполнить следующие действия:

- Загрузить ТС и нажать клавишу входа в BIOS. Во время запуска часто отображается экран с упоминанием клавиши для входа в BIOS. Если его нет или экран переключается слишком быстро, необходимо проверить сайт производителя материнской платы.
- После входа в BIOS найти раздел «Boot» или «Загрузка», где находятся все настройки, связанные с загрузкой компьютера.
- В разделе «Boot» найти опцию «Boot Mode» или «Режим загрузки» и выбрать «UEFI», чтобы включить его.
- В разделе «Boot» найти и деактивировать опцию безопасного запуска «Secure Boot», переведя ее в положение Disable (отключено).

- В разделе «Boot» выбрать загрузочное устройство с установочным образом **WAF Dallas Lock** первым в порядке загрузки, чтобы загрузка с него производилась раньше, чем с других загрузочных устройств;
- После включения режима UEFI сохранить изменения, выбрав опцию «Save and Exit», и подтвердить сохранение изменений. ТС перезагрузится, и загрузка будет производиться в режиме UEFI.

WAF Dallas Lock поставляется на CD-диске или в архиве поставки изделия в виде образа (*.iso), расположенного в каталоге **Distributives**.

Для установки **WAF Dallas Lock** необходимо:

1. Создать загрузочный внешний носитель с помощью специализированной утилиты или скопировать образ (*.iso) в файловую систему операционной системы.
2. Установить подготовленный внешний носитель в качестве загрузочного диска в BIOS ТС или установить скопированный образ (*.iso) в качестве загрузочного в параметрах виртуальной машины.
3. В загрузочном меню выбрать пункт **Install WAF DL 1.2.1**, чтобы начать установку продукта (см. Рисунок 3).

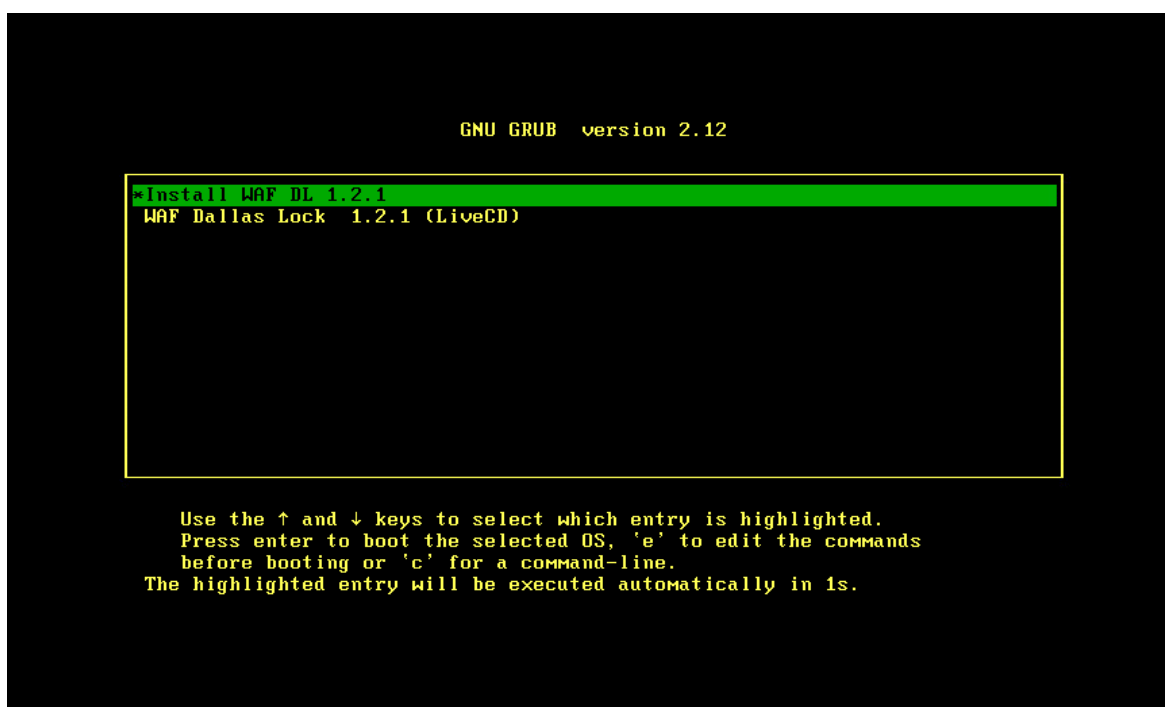


Рисунок 3. Загрузочное меню WAF Dallas Lock

4. После загрузки с загрузочного носителя или образа диска появится графическое меню, где выбрать диск, на который будет осуществляться установка **WAF Dallas Lock** (см. Рисунок 4).
5. Нажать кнопку **Установить** и в открывшемся окне подтвердить установку, нажав кнопку **Да**.



Другие системы на выбранном диске будут удалены.

6. Начнется процесс записи образа изделия на жесткий диск, необходимо дождаться завершения процесса установки.



Рисунок 4. Выбор диска

- По окончании процесса установки перезагрузить ТС, нажав кнопку **ОК** в появившемся окне (см. Рисунок 5).

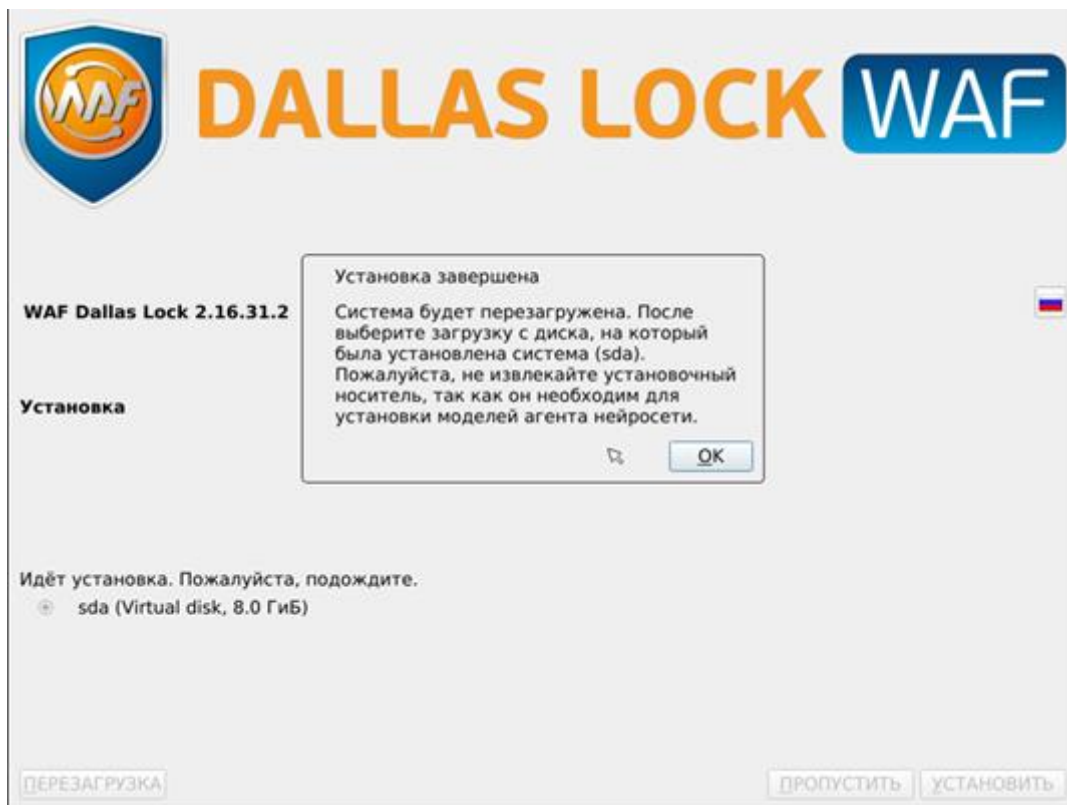


Рисунок 5. Перезагрузка

8. Когда перезагрузка завершится, в загрузочном меню выбрать **WAF Dallas Lock** и на экране **Настройка** (см. Рисунок 6) задать сетевое имя устройства, сконфигурировать LAN-интерфейс сервера (при необходимости активировать функцию DHCP-сервера для интерфейса), выбрать диск для хранения временных файлов и при необходимости его очистить.
9. После ввода всех настроек нажать кнопку **Применить**, среда исполнения продолжит загрузку и по завершении процесса будет готова к последующим настройкам.

)

Рисунок 6. Меню первоначальной настройки WAF Dallas Lock

- Сконфигурировать настройку сети вручную, например, задать маршрут до подсети управления и настроить сетевые интерфейсы можно, нажав кнопку **Дополнительные настройки сети** (см. Рисунок 7):
 - **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 применяться для настройки данной сетевой карты, где eth обозначает что используется Ethernet интерфейс, а 0 — номер устройства. Если установлено несколько сетевых устройств, то им будут присвоены имена eth0, eth1, eth2 соответственно.

The screenshot shows the WAF Dallas Lock configuration interface. A modal dialog box titled 'Дополнительные настройки сети' (Additional network settings) is open. It contains the following sections:

- Маршрут до подсети управления** (Management subnet route):
 - ☐ Задать маршрут до подсети управления (Set management subnet route)
 - Подсеть: [text input] / [text input]
 - Шлюз: [text input]
- Политики интерфейсов** (Interface policies):

Политика	Сетевой интерфейс
LAN	eth0 (MAC: 00:50:56:A2:BF:54)
WAN	eth1 (MAC: 00:50:56:A2:FF:F8)
DMZ	eth2 (MAC: 00:50:56:A2:14:10)

Below the dialog, the main configuration page is visible with fields for 'Имя хоста', 'Часовой пояс', 'Локальный IP-адрес' (192.168.1.1), 'Запустить DHCP-сервер', 'Диск для /var' (sda), and 'Очистить /var'. Buttons for 'ВЫХОД', 'ПРИМЕНИТЬ', 'ОК', and 'ОТМЕНА' are present.

Рисунок 7. Дополнительные настройки сети

2.5 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;
- обеспечить подключение между LAN-портом сервера (интерфейсом виртуальной машины) и компьютером;
- 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 пользователя с ролью *Администратор* (root) в текстовое поле *Имя пользователя*. Поле *Пароль*... необходимо оставить пустым. Нажать кнопку **Войти** (см. Рисунок 8);

The screenshot shows a light blue authentication form titled 'Выполните аутентификацию' (Perform authentication). It contains two input fields: the first has 'root' entered, and the second is labeled 'Пароль...' (Password...). At the bottom right are two buttons: 'Войти' (Login) in green and 'Сбросить' (Reset) in red.

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.

Настройки интерфейса управления WAF DL

Рисунок 9. Создание пароля администратора



Пароль должен соответствовать требованиям безопасности и содержать минимум 8 символов, включая:

- нижний регистр;
- верхний регистр;
- цифру;
- специальный символ.

2.6 Настройка перенаправления DNS-запросов

Правильная настройка DNS важна для обеспечения полной и эффективной работы модуля UTM. Необходимо в меню **Сеть** на странице *DHCP и DNS* заполнить поле *Перенаправление запросов DNS* адресами DNS-серверов (см. Рисунок 10).



Можно указывать как внешние, так и внутренние DNS-серверы. Например:

- внешний DNS сервер с адресом, например, 77.88.8.8, который будет использоваться для разрешения запросов к внешним ресурсам;
- внутренний DNS сервер для доменов в формате .local с адресом 10.10.10.10.

В поле *Перенаправление запросов DNS* необходимо указать следующий порядок серверов:

- внутренний DNS сервер: /local/10.10.10.10;
- внешний DNS сервер: 77.88.8.8.

Настройки сервера



Основные настройки

Дополнительные настройки

Требуется домен	☒
Авторизованный	☐
Локальный сервер	/lan/
Локальный домен	lan
Запись запросов	☐
Перенаправление запросов DNS	/local/10.10.10.10 - + 77.88.8.8 - +
Защита от DNS Rebinding	☒
Разрешить локальный хост	☒
Белый список доменов	ucc.local - +
Только локальный DNS	☒
Не использовать wildcard	☒
Интерфейс для входящих соединений	- +
Исключите интерфейсы	- +

Рисунок 10. Перенаправление запросов DNS

2.7 Лицензирование продукта

Для защиты от нелегального использования продукта необходимо загрузить файл лицензии **WAF Dallas Lock** (см. 5.4.1 Система).

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

2.8 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 11).

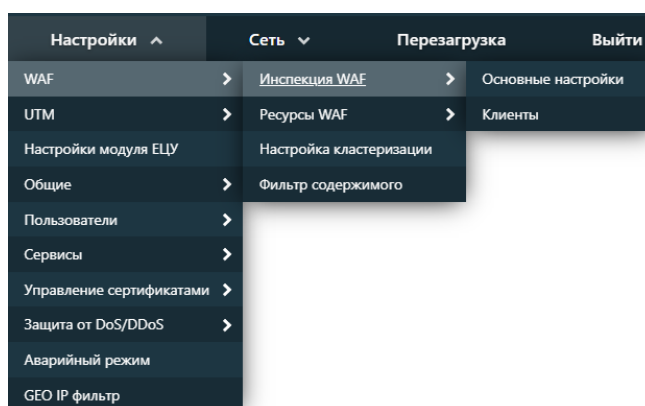


Рисунок 11. Инспекция WAF

На вкладке **Общие настройки** (см. Рисунок 12) включить инспекцию WAF и установить количество процессов, обслуживающих WAF в поле **CTF Очереди** и при необходимости разрешить HTTP соединения.

Инспекция WAF



Основные настройки

Клиенты

Включить	☒
СТФ Очереди	2 - по умолчанию ✓
Быстрый анализ HTTP-запросов	☒

Использовать нейросеть

Включить агента	☒
Количество потоков для нейросети	2 - по умолчанию ✓
Порог вероятности	90 % ✓

Точки входа

Включить HTTP	☒
HTTP порт	80 ✓
HTTPS порт	443 ✓
Доступная версия HTTP	HTTP/2
'Keep-Alive' или 'Close' соединения	http-keep-alive

Безопасное подключение

Мин уровень протокола TLS	TLS v1.2
Включить HSTS	☐

Сохранить

Применить

Сбросить

Рисунок 12. Инспекция WAF

Далее на странице *Ресурсы 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 13). Подробное описание функциональных возможностей настроек на вкладке *Защищаемые серверы* в разделе 5.1.2 Ресурсы WAF.

Ресурсы WAF



Защищаемые серверы

Защищаемые ресурсы

Настройки защищаемого сервера

Имя	node1
Тип сервера	Основной
IP-Адреса	172.16.157.10 ✓ − +
Тип распределения	roundrobin
Redispatch	☒
HTTP/WS	☒
Защита CSRF	☒
Временное окно для доступа к ЗР	600 ✓
Keep-Alive or Close connection	http-server-close
Расширенные настройки	☒
Тайм-аут сервера	20ms ✓
Тайм-аут подключений	20ms ✓
Тайм-аут состояния	20ms ✓
Check server	☒
Forward-For	☐
Описание	server.dl.local

Назад

Сохранить

Применить

Сбросить

Рисунок 13. Добавление защищаемого объекта

После сохранения защищаемый объект автоматически добавляется в список на вкладке *Защищаемые серверы* (см. Рисунок 14).

Ресурсы WAF

Защищаемые серверы

Защищаемые ресурсы

Имя	IP-Адреса	HTTP	Защита CSRF	Описание	
node1	172.16.157.10	☒	☐	server.dl.local	Изменить Удалить

Добавить +

Сохранить

Применить

Сбросить

Рисунок 14. Список защищаемых объектов

После того как добавили защищаемый ресурс, нужно перейти в **Настройки — WAF — Ресурсы WAF — Защищаемые ресурсы** и добавить корневой сертификат Удостоверяющего центра (см. Рисунок 15). Более подробное описание настройки смотреть в разделе [5.1.2 Ресурсы WAF](#).

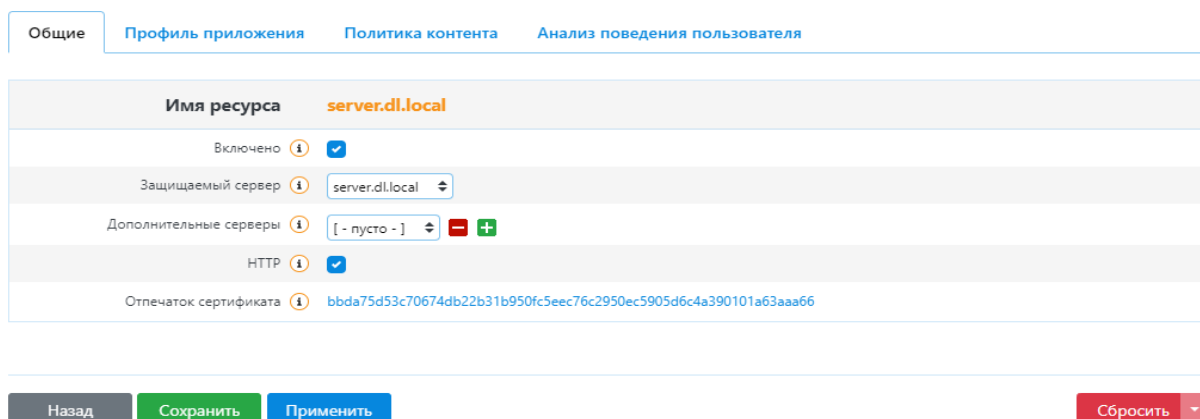


Рисунок 15. Добавление сертификата

Далее на вкладке *Профиль приложения* можно задать механизмы защиты защищаемого ресурса.

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;
- обеспечить IP-соединение веб-сервера и интерфейса DMZ **WAF Dallas Lock**;



По умолчанию для интерфейса DMZ установлен адрес 172.16.16.1 и маска подсети 255.255.255.0. При необходимости внести изменения в конфигурацию интерфейса можно в графической консоли администрирования, в меню **Сеть — Интерфейсы — DMZ** (более подробно в разделе [6.1 Интерфейсы](#)).

- на странице **Сеть — Имена хостов** 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 WAN и DMZ-зоны;
- отображение веб-страницы, передаваемой веб-сервером, обращением со стороны хоста из LAN-зоны по IP-адресу веб-сервера в DMZ.



Доступ к защищаемому ресурсу по протоколу HTTPS осуществляется по IP-адресу WAN-интерфейса **WAF Dallas Lock** без указания порта 7443. Для подключения к защищаемому ресурсу по сетевому имени необходимо настроить необходимые параметры на DHCP-сервере или локально в файле hosts.

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.

Учитывая, что WAF и UTM являются отдельно лицензируемыми модулями, пользователям отображаются только те виджеты, модули которых были лицензированы.

На виджетах с графиками и кольцевыми диаграммами реализована возможность выборки по диапазону дат. Для изменения периода необходимо нажать кнопку **За сегодня** и выбрать период (1 час, 3 часа, 6 часов, 12 часов или 24 часа) или кнопку **Все записи** и на полосе отображения дат выбрать необходимый период.

При применении какой-либо выборки на одном из следующих виджетов: **Атакуемые ресурсы**; **Все зафиксированные атаки**; **Источники атак**; **Уровни тревоги атак** ее результаты автоматически применяются на остальных перечисленных виджетах.

При применении какой-либо выборки на одном из следующих виджетов: **Атаки, зафиксированные на ресурсы**; **Источники атак, зафиксированные на ресурсы**; **Уровни тревоги атак, зафиксированные на ресурсы** ее результаты автоматически применяются на остальных перечисленных виджетах.

3.1 Виджет «Атакуемые ресурсы»

Виджет с кольцевой диаграммой, на котором отображены наиболее атакуемые ресурсы из списка защищаемых (см. Рисунок 16).

При нажатии на какой-либо ресурс, он отображается на виджете **Атаки, зафиксированные на ресурсы**. На виджете **Атакуемые ресурсы** может отображаться не более 10 записей, цвет сектора диаграммы соответствует цвету атакуемого ресурса в легенде.

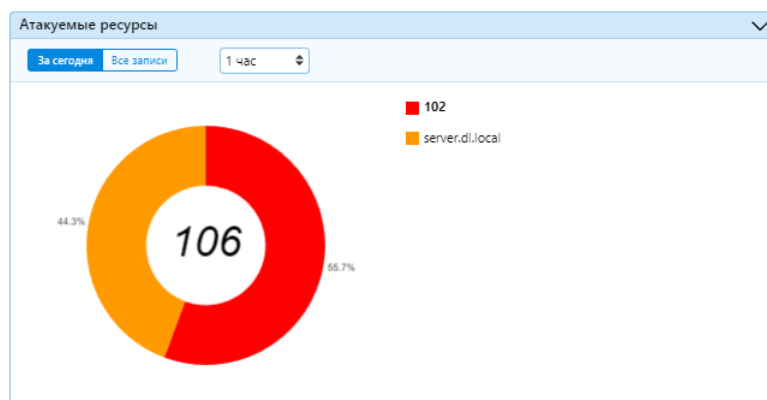


Рисунок 16. Виджет «Атакуемые ресурсы»

3.2 Виджет «Аппаратное обеспечение»

Виджет **Аппаратное обеспечение** (см. Рисунок 17) 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.

На данном виджете отображаются следующие данные:

- *Процессор.* Динамически изменяемый индикатор (прогресс-бар) загрузки процессора и его значение в процентах;
- *ОЗУ.* Динамически изменяемый индикатор (прогресс-бар) используемой оперативной памяти и текстовая запись в виде «занято памяти/всего памяти [занято памяти в процентах]» в гигабайтах (мегабайтах);
- *Использование диска.* Динамически изменяемые индикатор (прогресс-бар) заполненности диска и текстовая запись в виде «занято места на диске/всего места на диске [занято места в процентах]» в гигабайтах (мегабайтах);
- *Средняя нагрузка.* Динамически изменяемые текстовые записи вида «средняя загрузка системы за 1 минуту, 5 минут и 15 минут».

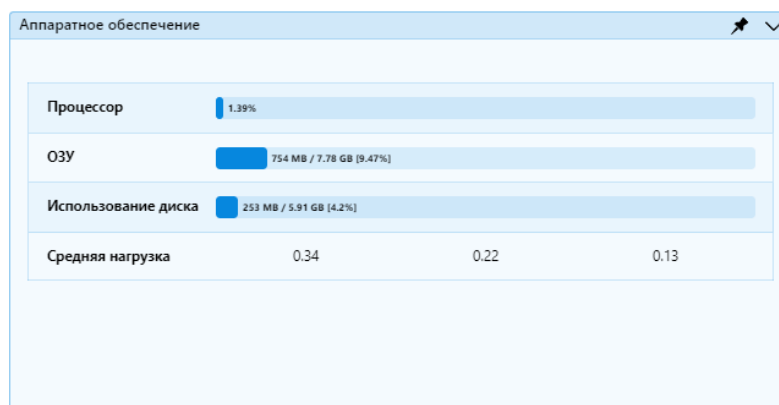


Рисунок 17. Виджет «Аппаратное обеспечение»

3.3 Виджет «Все зафиксированные атаки»

Виджет с кольцевой диаграммой (см. Рисунок 18), на котором отображены девять наиболее массовых (по количеству) атак, обнаруженных МЭ уровня веб-сервера (тип Г), на все защищаемые ресурсы.

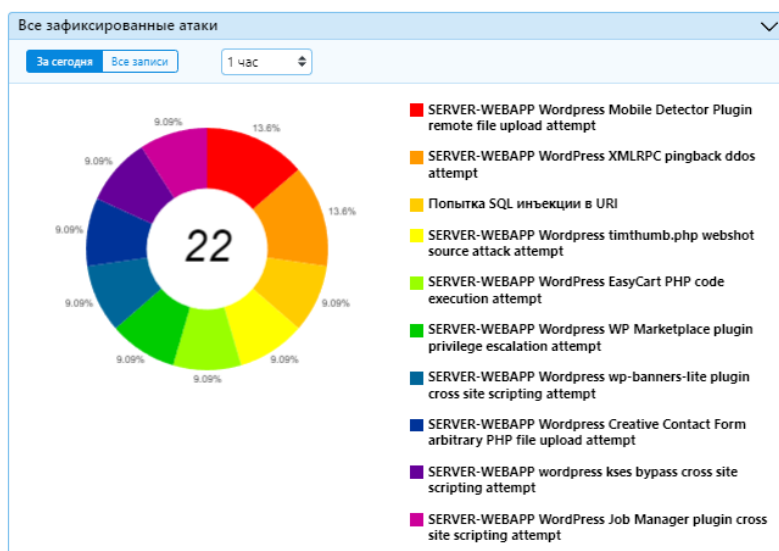


Рисунок 18. Виджет «Все зафиксированные атаки»

3.4 Виджет «Источники атак»

Виджет с кольцевой диаграммой, на котором отображены источники всех зафиксированных атак (см. Рисунок 19).

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.

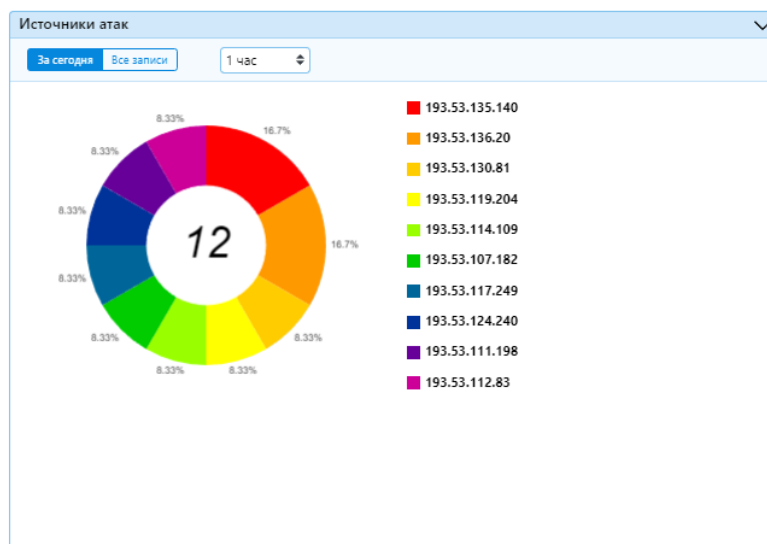


Рисунок 19. Виджет «Источники атак»

3.5 Виджет «Атаки, зафиксированные на ресурсы»

Виджет содержит кольцевую диаграмму с источниками, по которым выводятся атаки. Наблюдаемые ресурсы указываются вручную или при помощи кнопки **Добавить ресурсы** или **Изменить ресурсы**, если ранее были выбраны наблюдаемые ресурсы (см. Рисунок 20).

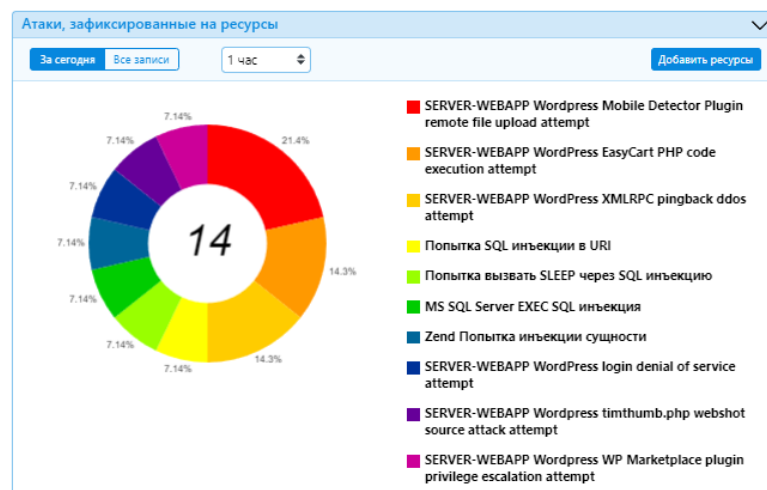


Рисунок 20. Виджет «Атаки, зафиксированные на ресурсы»

В окне выбора защищаемых ресурсов для отображения на виджете необходимо отметить соответствующие чекбоксы напротив имен защищаемых ресурсов и подтвердить выбор кнопкой **Сохранить**, для очистки выбора необходимо нажать кнопку **Очистить** (см. Рисунок 21).

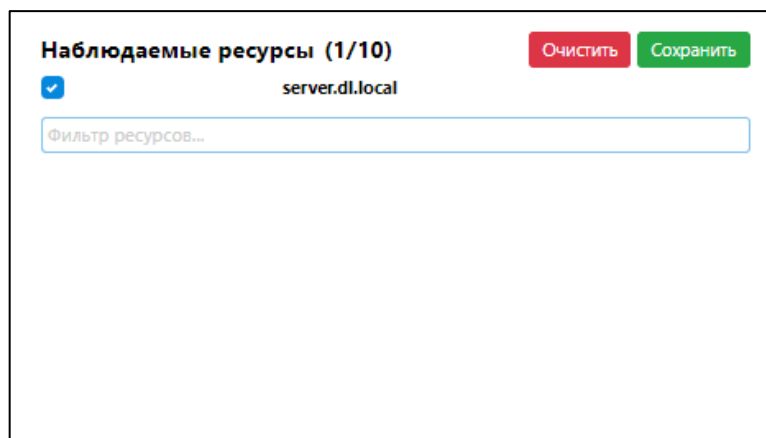


Рисунок 21. Окно «Наблюдаемые ресурсы»

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 22).

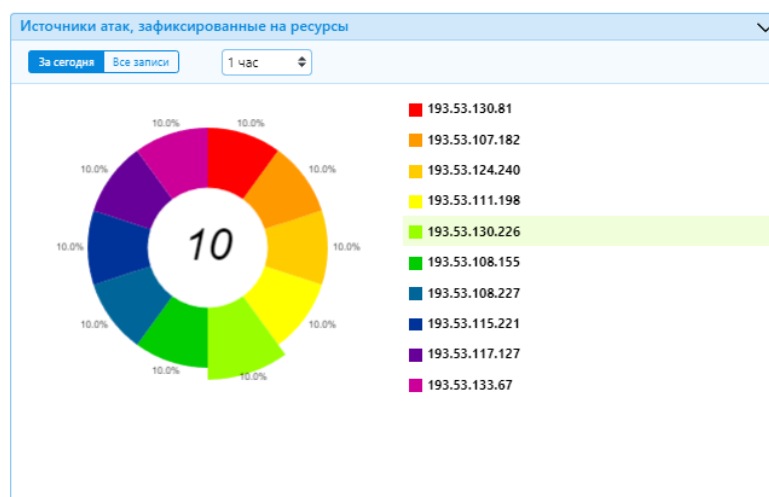


Рисунок 22. Виджет «Источники атак, зафиксированные на ресурсы»

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 (см. Рисунок 23).

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.

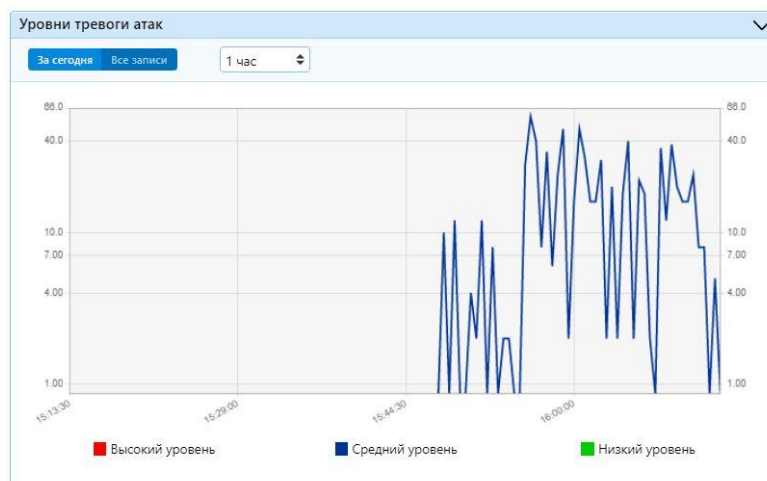


Рисунок 23. Виджет «Уровни тревоги атак»

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*.

Данный виджет содержит не более десяти защищаемых ресурсов. Удаление ресурса из списка наблюдаемых происходит путем нажатия кнопки **Изменить ресурсы** и выключением чекбокса напротив его имени (при этом кольцевая диаграмма будет перестроена). 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 24).

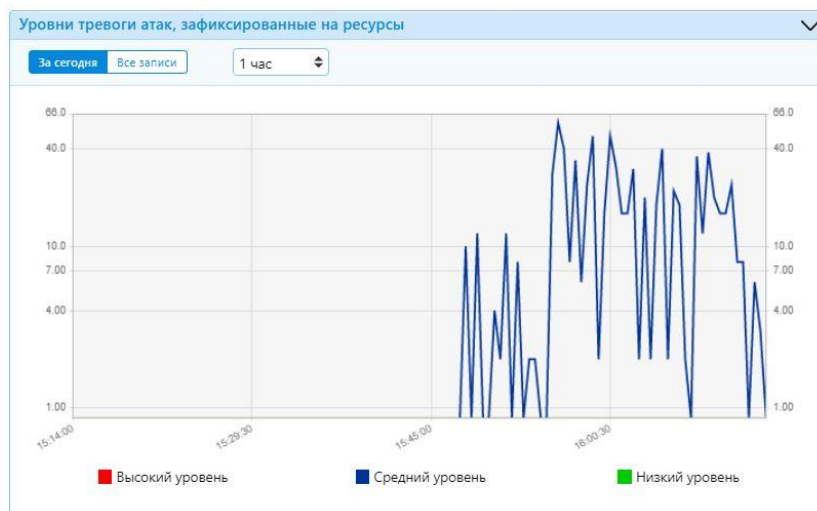


Рисунок 24. Виджет «Уровни тревог атак, зафиксированные на ресурсы»

3.9 Блок «Список инцидентов»

Блок **Список инцидентов** (см. Рисунок 25) должен содержать в себе зафиксированные данные по инцидентам безопасности, относящимся только к событиям МЭ уровня веб-сервера (тип 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.
- Дата и 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.

ID	Дата и время	Событие	Информация
8197	28.03.2025 16:10:29	[2] Forbidden command GET	Блокировка IP - 192.168.131.81

Рисунок 25. Блок «Список инцидентов»

3.10 Виджет «Трафик в реальном времени»

Виджет **Трафик в реальном времени** представлен в виде графика входящего и исходящего, входящего или исходящего трафика по защищаемым ресурсам (см. Рисунок 26).

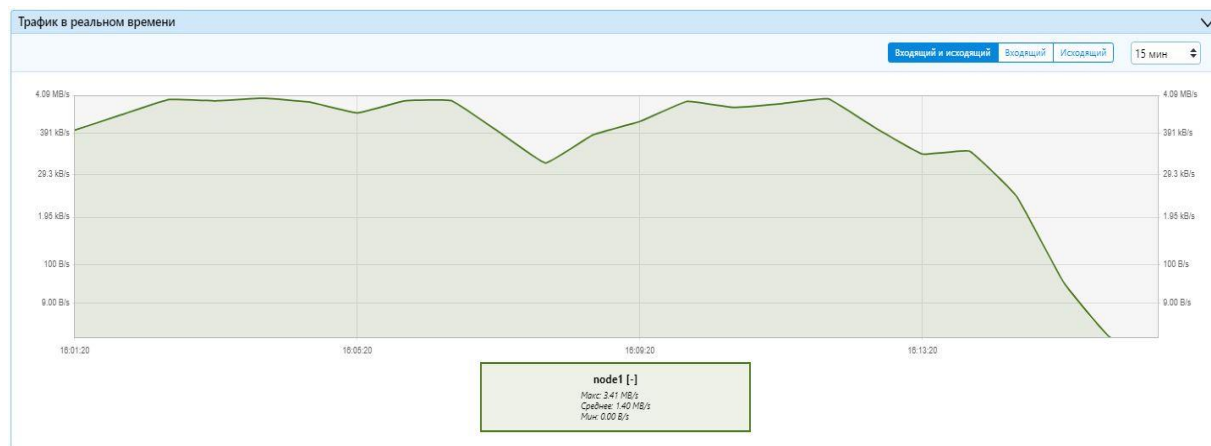


Рисунок 26. Виджет «Трафик в реальном времени»

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 27) 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 27. Виджет «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 28), 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 межсетевого экрана уровня веб-сервера, основанные на: сигнатурном анализе правил для межсетевого экрана уровня веб-сервера; анализе поведения пользователей нейронными сетями; сравнении действий пользователей с параметрами графа связей.
- Журнал *COB* — 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 логических границ 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 события режима усиленной защиты от DoS/DDoS атак.
- Журнал *Прокси* — отображает данные как по HTTP-запросам к веб-серверу, так и по ответам, полученным от веб-сервера.

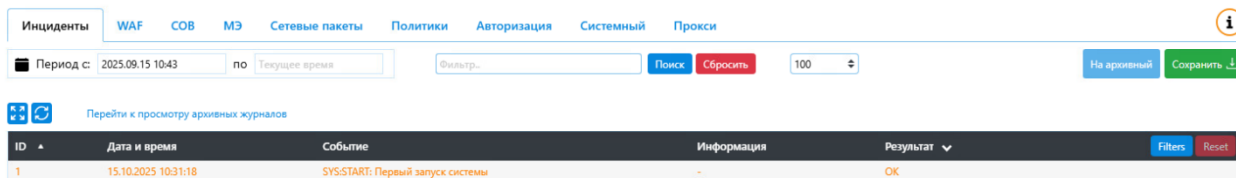


Рисунок 28. Журналы аудита

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 COB 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 *Политики*.

Сбой журналирования системы заносится в *Системный* журнал.

4.1.2 Содержание журналов аудита

Каждый журнал аудита содержит набор полей, в которые вносятся данные, относимые к тому или иному событию. Для каждого журнала список полей отличается (см. Таблица 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 Правило № Результат Информация
COB	ID — уникальный номер записи журнала (идентификатор события) Дата и время Событие Источник Направление Протокол Правило № Результат Информация
МЭ	ID — уникальный номер записи журнала (идентификатор события) Дата и время Событие Источник Направление Протокол Правило №

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

Наименование журнала	Список полей
	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 ниже (см. Таблица 2).

Таблица 2. Список журналируемых событий

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

Наименование журнала	Список событий
	Блокировка перехода на защищаемом ресурсе графом связи Обнаружение аномальной активности нейронными сетями
COB	Срабатывание правил эвристического анализа COB Срабатывание правил COB
МЭ	Срабатывание правил 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 Включение или отключение автозапуска служб
Авторизация	Вход/выход учетной записи пользователя Получение прав администрирования Изменение паролей пользователей
Системный	События системного журнала SysLog События по запуску/остановке процессов в автоматическом режиме События запуска/остановки/перезагрузки процессов по команде администратора 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

Для журналов *WAF*, *COB* и *МЭ* есть возможность перехода к просмотру параметров сработавшего правила, для этого необходимо нажать на номер правила в колонке *Правило №*. Кроме этого, для журнала *WAF* есть возможность (см. Рисунок 29):

- перехода в журнал *Прокси* с выбранным источником атак, для этого необходимо нажать на адрес атакующего в колонке *Источник*;
- просмотра IP-адреса атакующего из заголовка пакета в колонке *Информация*.

ID	Дата и время	Событие	Источник	Направление	Протокол	Правило №	Результат	Информация
2	15.10.2025 10:31:59	Self-test Body test	192.168.130.115:80	192.168.13.46:39130	TCP	[WAF-0992:3]	OK	Classification: A.suspicious.string.was.detected
1	15.10.2025 10:31:59	Self-test Header test	192.168.13.46:39130	192.168.130.115:80	TCP	[WAF-0991:3]	OK	Classification: A.suspicious.string.was.detected

Рисунок 29. Записи в журнале WAF

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 30).

Во всех журналах предусмотрена возможность:

- поиска;
- выбора количества отображаемых событий на странице (от 25 до 500);
- выбора отображаемого периода² (см. Рисунок 30);
- фильтрации по определенным столбцам;
- сортировки по столбцам (по убыванию и возрастанию).

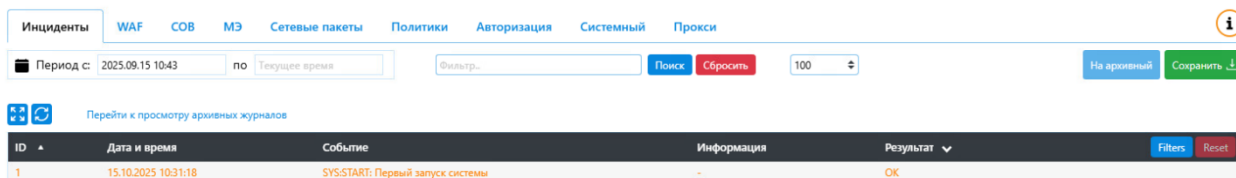


Рисунок 30. Количество отображаемых событий и выбор периода

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 31).

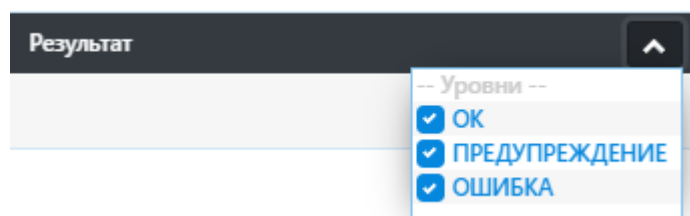


Рисунок 31. Фильтрация и отображение событий

В журнале *Прокси* по умолчанию отображаются все события. Чтобы в списке отображались только запросы с ошибками и предупреждениями, необходимо включить переключатель в режим *Только ошибки* (см. Рисунок 32).

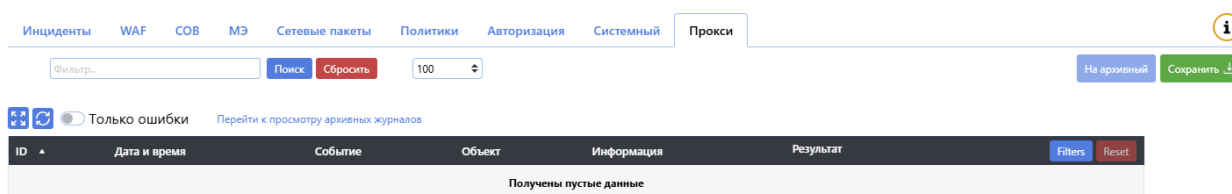


Рисунок 32. Отображение списка ошибок и предупреждений

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 **Сохранить**. Факт выгрузки активного журнала фиксируется в *Системном* журнале.

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

² За исключением журнала *Прокси*.

4.2 Журнал ядра

Страница (см. Рисунок 33) 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.

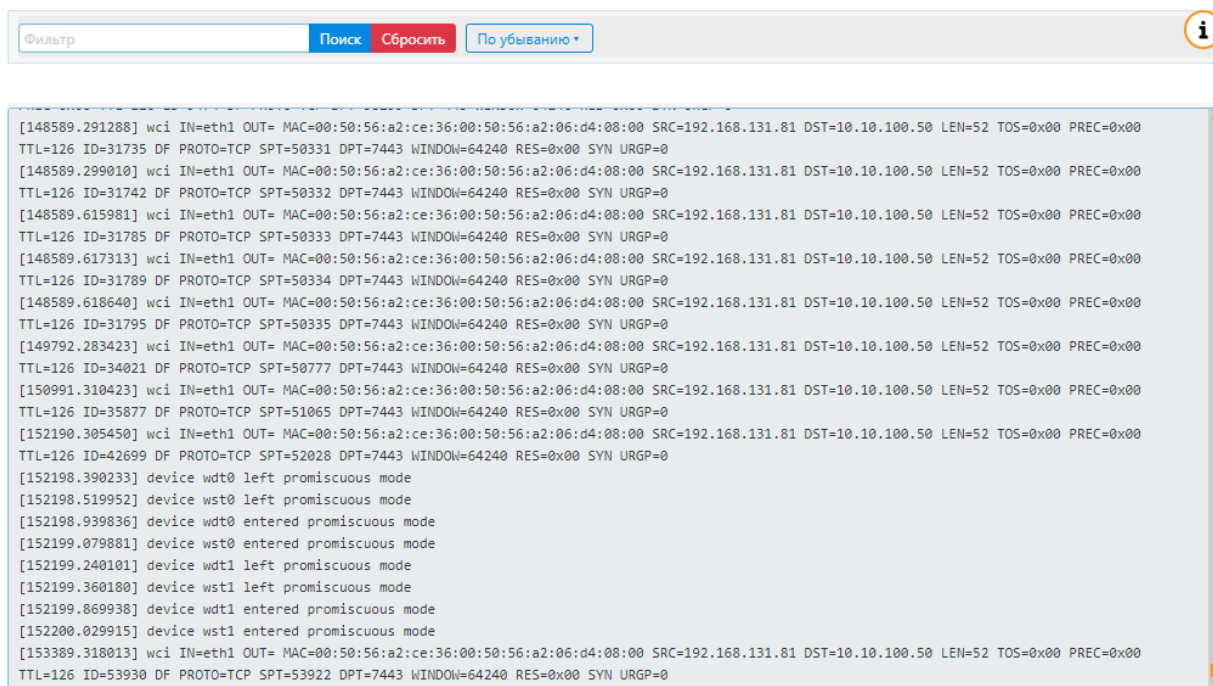


Рисунок 33. Журнал ядра

4.3 Журналы аварийного режима

Журнал аварийного режима (см. Рисунок 34) является техническим, он не содержит обязательных полей, таких как идентификатор события, дата, результат.

В системе хранится всегда две разные 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 (выполнения команд из командной строки) до момента выхода из аварийного режима.

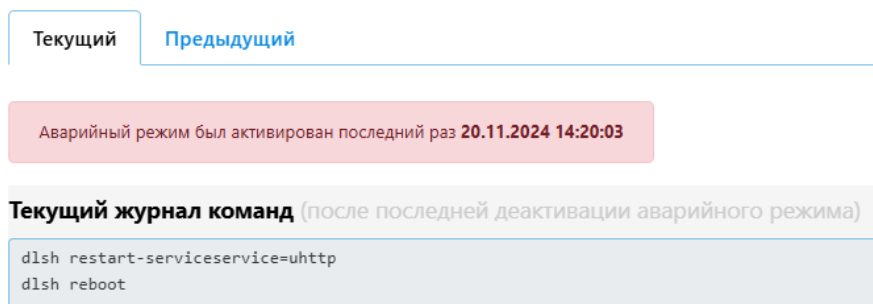


Рисунок 34. Журнал аварийного режима

4.4 Сеть

4.4.1 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 35) 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.

☐ TCP ☐ UDP ☒ Соединения ☐ Ожидание соединений ☐ Все ☐ Символьные имена

Таблица: tcp

Протокол	Очереди приема	Очереди отправки	Локальный адрес	Удалённый адрес	Состояние	PID
tcp	0	0	10.10.100.50:7443	192.168.131.81:59056	TIME_WAIT	-
tcp	0	0	10.10.100.50:7443	192.168.131.81:59063	TIME_WAIT	-
tcp	0	0	127.0.0.1:1883	127.0.0.1:55370	ESTABLISHED	3396/mosquitto
tcp	0	0	10.10.100.50:7443	192.168.131.81:58996	TIME_WAIT	-
tcp	0	0	192.168.1.250:49810	192.168.1.250:7883	ESTABLISHED	4241/octopus
tcp	0	0	127.0.0.1:51478	127.0.0.1:1883	ESTABLISHED	4241/octopus
tcp	0	0	10.10.100.50:7443	192.168.131.81:59061	TIME_WAIT	-
tcp	0	0	10.10.100.50:7443	192.168.131.81:58933	TIME_WAIT	-

Рисунок 35. Сетевая статистика

4.4.2 Состояние межсетевого экрана

На данной странице (см. Рисунок 36) представлены таблицы IPTABLES (Filter, NAT, Mangle, Raw) по протоколам IPv4 и IPv6, а также реализованы кнопки управления: **Сбросить счетчики** и **Перезапустить межсетевой экран**.

Межсетевой экран IPv4

Межсетевой экран IPv6

Таблица: Filter

Сбросить счётчики

Перезапустить межсетевой экран

Цепочка INPUT (Политики: ACCEPT, Пакеты: 0, Трафик в реальном времени: 0.00 B)

Пакетов	Трафик в реальном времени	Назначение	Протокол	В	Вне	Источник	Направление	Опции
118	11.79 KB	ACCEPT	tcp	*	*	0.0.0.0/0	192.168.1.0/24	tcp dpt:7883
24	960.00 B	ACCEPT	112	*	*	0.0.0.0/0	224.0.0.18	-
242	59.85 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	/* !fw3 */
1167	298.15 KB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	/* !fw3: Custom input rule chain */
13	780.00 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED /* !fw3 */
0	0.00 B	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:443 /* !fw3: wproxy_https */
0	0.00 B	ACCEPT	udp	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:443 /* !fw3: wproxy_http3 */
0	0.00 B	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:80 /* !fw3: wproxy_http */
0	0.00 B	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	/* !fw3 */
30	2.61 KB	zone_wan_input	all	eth1	*	0.0.0.0/0	0.0.0.0/0	/* !fw3 */
3	108.00 B	zone_dmz_input	all	eth2	*	0.0.0.0/0	0.0.0.0/0	/* !fw3 */

Рисунок 36. Состояние межсетевого экрана

4.4.3 Маршруты

На странице (см. Рисунок 37) 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.

ARP

IPv4-Адрес	MAC-Адрес	Интерфейс
192.168.157.10	00:50:56:a2:1f:eb	br-lan
10.10.100.1	00:50:56:a2:06:d4	eth1
172.16.157.10	00:50:56:a2:8d:27	eth2
192.168.157.101	00:50:56:a2:a9:17	br-lan

Active IPv4-Маршруты

Сеть	Назначение	IPv4-Шлюз	Метрика	Таблица
wan	0.0.0.0/0	10.10.100.1	0	main
wan	10.10.100.0/22		0	main
dmz	172.16.157.0/24		0	main
lan	192.168.1.0/24		0	main
lan	192.168.157.0/24		0	main

Active IPv6-Маршруты

Сеть	Назначение	Источник	Метрика	Таблица
dmz	fd3a:b28b:a96b::/64		1024	main
lan	fd3a:b28b:a96b:1::/64		1024	main

IPv6 Neighbours

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

Рисунок 37. Маршруты

4.5 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 38) 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 38. Загрузка в реальном времени

В графике **Трафик в реальном времени** (см. Рисунок 39) отображается информация о загрузке трафика сети за выбранный период. 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.

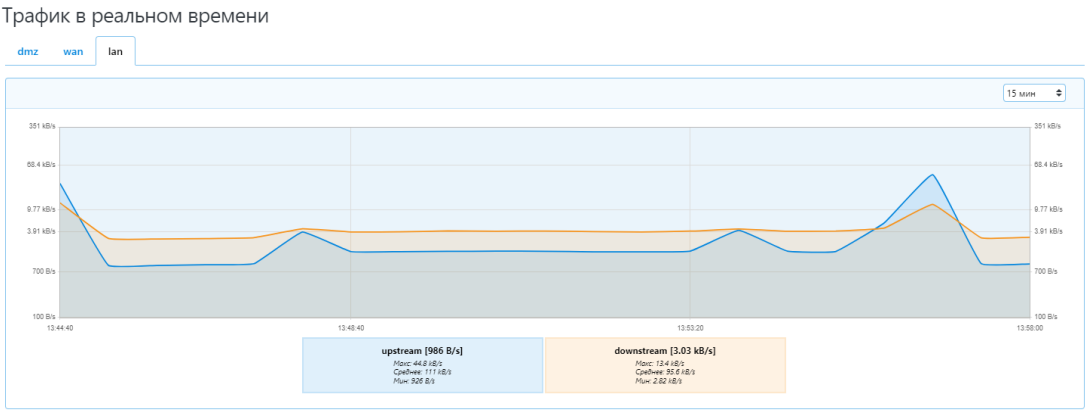


Рисунок 39. Трафик в реальном времени

Страница **Соединения в реальном времени** (см. Рисунок 40, Рисунок 41) 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.

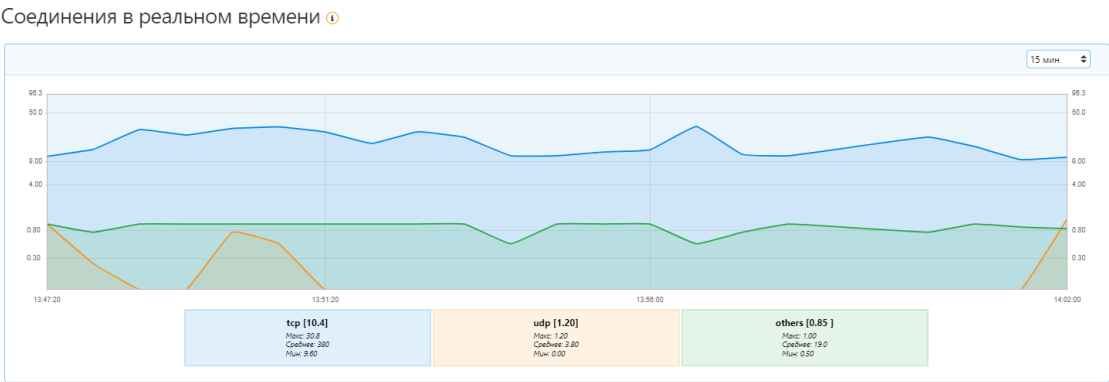


Рисунок 40. Соединения в реальном времени (график активных соединений)

Сеть	Протокол	Источник	Направление	Передача
IPV4	TCP	192.168.1.250:49798	192.168.1.250:7883	18.18 KB (160 Пакетов)
IPV4	TCP	192.168.1.250:49804	192.168.1.250:7883	15.25 KB (105 Пакетов)
IPV4	TCP	192.168.1.250:49852	192.168.1.250:7883	8.82 KB (68 Пакетов)
IPV4	TCP	192.168.1.250:49862	192.168.1.250:7883	5.83 KB (23 Пакетов)
IPV4	TCP	192.168.1.250:49844	192.168.1.250:7883	5.83 KB (23 Пакетов)
IPV4	TCP	192.168.1.250:49810	192.168.1.250:7883	5.83 KB (23 Пакетов)
IPV4	TCP	192.168.1.250:49834	192.168.1.250:7883	5.83 KB (23 Пакетов)

Рисунок 41. Соединения в реальном времени (таблица активных соединений)

4.6 Процессы

На данной странице (см. Рисунок 42) 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.

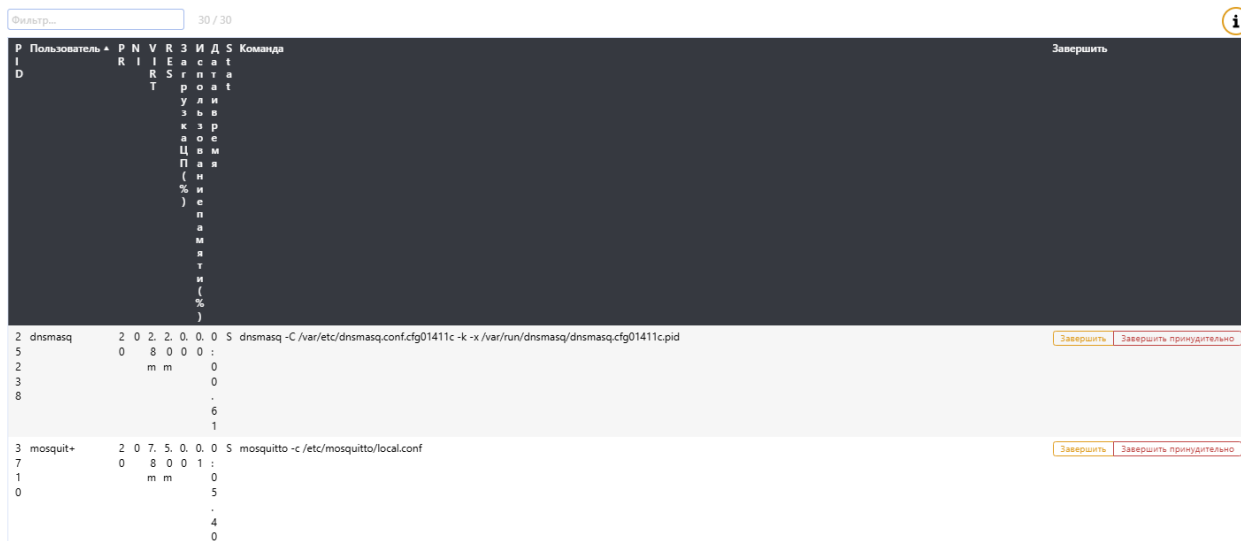


Рисунок 42. Процессы

4.7 Сведения о системе

На данной странице (см. Рисунок 43) представлены общие данные о системе.

Раздел Система содержит:

- **Имя хоста WAF Dallas Lock.**
- **Модель.** Наименование аппаратной платформы, на которую установлен **WAF Dallas Lock**. В случае использования виртуальной машины указывается виртуальная машина.
- **Система выпущена.** Ссылка на информационный ресурс компании, где можно найти информацию о продукте и другие предоставляемые услуги.
- **Версия прошивки.** Актуальная версия **WAF Dallas Lock**.
- **Версия ядра.** Версия операционной системы.
- **Номер лицензии.** Текущий номер лицензии продукта (содержится в файле лицензии).
- **Код поддержки.** Уникальный идентификационный номер, предоставляемый клиентам для доступа к технической поддержке (содержится в файле лицензии).
- **Дата и время.** Текущая дата и время.
- **Время работы.** Время непрерывной работы.
- **Средняя нагрузка.** Данные в реальном времени о средней нагрузке на систему.

Виджет **Оперативная память (RAM)** отображает в реальном времени размер свободного места в оперативной памяти и буферизацию.

Виджет **Использование диска** отображает в реальном времени общее свободное пространство на жестких дисках.

Виджет **Сеть** отображает данные о состоянии сети, содержащие сведения 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.

В случае возникновения ошибок в работе **WAF Dallas Lock** существует возможность сохранения всех параметров системы для передачи в службу технической поддержки, для этого необходимо нажать на ссылку **Скачать архив конфигурации для службы поддержки**.

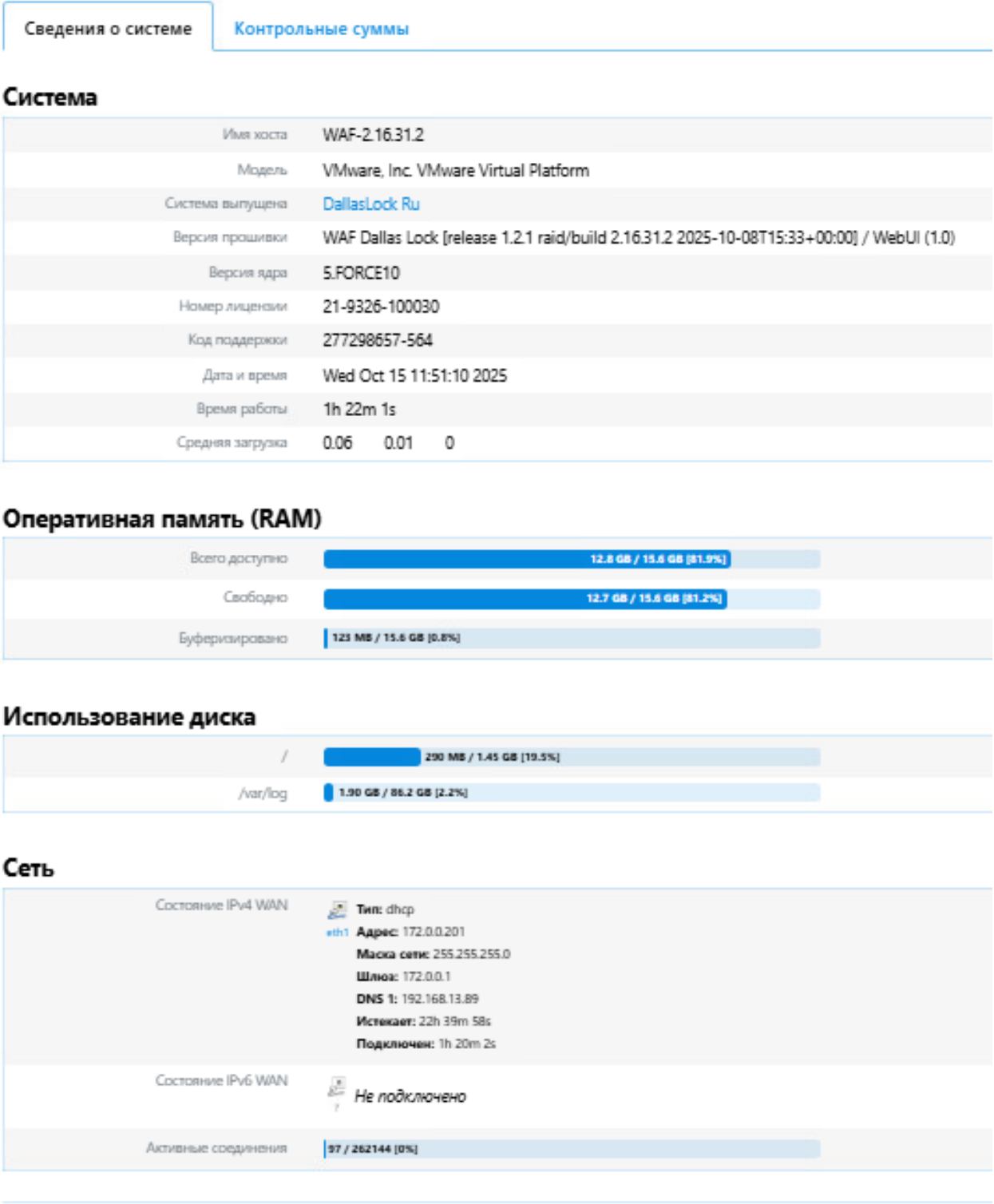


Рисунок 43. Страница «Сведения о системе»

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.

Сведения о системе		Контрольные суммы	
Контрольная сумма	Файл	Пересчитать КС	Скачать ↴
288319940660d3b9991aa80552236e39554e84c6bbfa197e971de18f631f8871	/usr/sbin/haproxy		
23f90598c000380636e54016c2f1682856bd241bc9c9f594a7684f53e7883ab5	/usr/sbin/wctf		
3c69e45efc0983882bee2358b8bd8498409aa1373bd3d156d098ef8730995703	/usr/sbin/tctf		
0c8bf5a2077f66928484224ebc6ae541f55f915cb7dc25e43e514f24e06bc418	/usr/sbin/octopus		
4dc492ab502ed6f8ed2f32edc6e0f1d88fbd52050ca4701484b1efdce1262cdd	/usr/lib/luajit/libluajit.so		
11be00562d7963a45281da16008e75717931681ebc6f16074c73849eb74af98e	/usr/lib/libres_mapping.so		
a82d5719c560a80ee6b4b650cd2dbd167f95e83c4e54e68df809a816d5b3f18c	/usr/bin/res_mapper		

Рисунок 44. Контрольные суммы

5 НАСТРОЙКА WAF DALLAS LOCK

Основной инструмент администратора **WAF Dallas Lock** — раздел меню **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 пункты меню второго уровня:

- WAF;
- UTM;
- Настройки модуля **ЕЦУ**;
- Общие;
- Пользователи;
- Сервисы;
- Управление сертификатами;
- Защита от DoS/DDoS;
- Аварийный режим;
- GEO IP фильтр.

Настройки ^	Сеть v	Перезагрузка
WAF >	Инспекция WAF >	Основные настройки
UTM >	Ресурсы WAF >	Клиенты
Настройки модуля ЕЦУ >	Настройка кластеризации	
Общие >	Фильтр содержимого	
Пользователи >		
Сервисы >		
Управление сертификатами >		
Защита от DoS/DDoS >		
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;
- Ресурсы WAF;
- Настройка кластеризации;
- Фильтр содержимого.

5.1.1 Инспекция WAF

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

- Основные настройки;
- 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 анализ содержимого ответа сервера контент-фильтром не осуществляется).



В **WAF Dallas Lock** реализована возможность анализа входящего трафика и обнаружения вторжений при помощи нейронных сетей, для следующих типов атак:

- внедрение SQL-кода (SQL-injection);
- межсайтовый скриптинг (Cross-site scripting, XSS);
- включение локального файла (Local File Inclusion, LFI);
- инъекция команд операционной системы (OS command injection).

Результаты, полученные при анализе входящего трафика с использованием нейронных сетей, записываются в журнал WAF.

В блоке **Использовать нейросеть** (см. Рисунок 46) доступны настройки нейронной сети.

- *Включить агента.* При включенном чекбоксе активируется анализ трафика посредством нейронных сетей, также становятся доступными следующие настройки:
 - *Количество потоков для нейросети.* Параметр позволяет выбрать количество процессов, которые будут использоваться при анализе трафика с использованием нейронных сетей.
 - *Порог вероятности.* Поле позволяет установить значение пороговой вероятности в процентах, при которой нейросеть посчитает подозрительные действия атаккой.

Нейронные сети работают совместно с фильтром содержимого WAF, анализируя трафик и принимая решение о блокировке следующим образом:

- Если и фильтр содержимого WAF, и нейронные сети обнаруживают угрозу, то блокировка осуществляется с помощью правила фильтра содержимого WAF.
- Если только фильтр содержимого WAF выявляет угрозу, а нейронные сети — нет, блокировка все равно производится с помощью фильтра содержимого WAF.
- Если атака выявлена только нейронными сетями, но не зафиксирована фильтром содержимого WAF, и вероятность превышает установленный порог, то блокировка не производится, а информация записывается в журналы аудита.



Нейронные сети уведомляет администратора о событиях безопасности, не блокируя при этом возможные атаки. Если в журналах аудита обнаружено, что какой-то IP-адрес совершает подозрительную активность и не был заблокирован автоматически другими механизмами **WAF Dallas Lock**, администратор может вручную добавить этот адрес в список заблокированных (более подробно в пункте [6.5.5 Списки доступа МЭ](#)).

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

- *Включить HTTP.* При включенном чекбоксе разрешается HTTP-соединение, также становятся доступными следующие настройки:
 - *HTTP порт.* Поле позволяет изменить порт HTTP (по умолчанию 80);
 - *HTTPS порт.* Поле позволяет изменить порт HTTPS (по умолчанию 443).



Для изменения HTTP и HTTPS портов необходимо также изменить порты в правилах *wproxy_https*, *wproxy_http3*, *wproxy_http* межсетевого экрана (см. [6.5.3 Правила для трафика](#)), HTTP и SSL-порты в настройках переменных фильтра содержимого (см. [5.4.5 Фильтр содержимого](#)).

- *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** — задает время, указанное в секундах, в течение которого доступ к сайту должен осуществляться только по протоколу HTTPS. Значение по умолчанию — 16000000s.

Инспекция WAF



Основные настройки

Клиенты

Включить ☒

CTF Очереди ⓘ

2 - по умолчанию ✓ ↕

Быстрый анализ HTTP-запросов ⓘ

☒

Использовать нейросеть ⓘ

Включить агента ☒

Количество потоков для нейросети

2 - по умолчанию ✓ ↕

Порог вероятности

90 ✓ %

Точки входа

Включить HTTP ☒

HTTP порт

80 ✓

HTTPS порт

443 ✓

Доступная версия HTTP ⓘ

HTTP/2 ↕

'Keep-Alive' или 'Close' соединения ⓘ

http-keep-alive ↕

Безопасное подключение

Мин уровень протокола TLS ⓘ

TLS v1.2 ↕

Включить HSTS ⓘ

☐

Сохранить

Применить

Сбросить ▾

Рисунок 46. Инспекция WAF. Основные настройки

На вкладке *Клиенты* (см. Рисунок 47) загружаются корневой сертификат Удостоверяющего центра (УЦ), список отозванных сертификатов УЦ и клиентские сертификаты для функции ограничения доступа к защищаемому ресурсу с использованием клиентских сертификатов. Корневые сертификаты и список отозванных сертификатов можно добавить либо с помощью файла, либо указать URL источника.

Инспекция WAF

Основные настройки

Клиенты

Включить аутентификацию по CA☒

Получить CA из

URL

CA URL

Получить список отзывов сертификатов из

URL

CRL URL

Автообновление списка отзыва сертификатов

☐

Общее имя

Серийный номер

Получить из файл сертификата

- На данный момент список пуст -

Добавить +

Сохранить

Применить

Сбросить

Рисунок 47. Инспекция WAF. Клиенты

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 при необходимости производится для указания источника списка отозванных сертификатов, соответствующего УЦ. Также существует возможность автоматического обновления списка отозванных сертификатов УЦ, при условии указания URL на необходимый список.

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 inspected 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 [5.4.2.2 Web-интерфейс](#).
- На каждой inspected станции необходимо установить следующие ключи: корневой сертификат УЦ, открытый ключ **WAF Dallas Lock** и пару открытый/закрытый ключ для inspected сервера/хоста.

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

5.1.2 Ресурсы WAF

На вкладке *Защищаемые серверы* (см. Рисунок 48) отображается список объектов, которые находятся под защитой **WAF Dallas Lock**. В любой момент можно внести новые объекты либо изменить существующие согласно разделу [2.8 Добавление защищаемого ресурса](#).

Ресурсы WAF

Защищаемые серверы

Защищаемые ресурсы

Имя

IP-Адреса

HTTP

Защита CSRF

Описание

node1

172.16.157.10

☒

☐

server.dl.local

Изменить

Удалить

Добавить +

Сохранить

Применить

Сбросить

Рисунок 48. Инспекция WAF. Защищаемые серверы

Вкладка *Защищаемые серверы* (см. Рисунок 49) позволяет произвести настройки для сервера, который вводится или уже введен под защиту **WAF Dallas Lock**.

Ресурсы WAF

[Защищаемые серверы](#)[Защищаемые ресурсы](#)

Настройки защищаемого сервера

Имя	node1
Тип сервера	Основной
IP-Адреса	172.16.157.10
Тип распределения	roundrobin
Redispatch	☒
HTTP/WS	☒
Защита CSRF	☒
Временное окно для доступа к ЗР	600
Keep-Alive or Close connection	http-server-close
Расширенные настройки	☒
Тайм-аут сервера	20ms
Тайм-аут подключений	20ms
Тайм-аут состояния	20ms
Check server	☒
Forward-For	☐
Описание	server.dl.local

[Назад](#) [Сохранить](#) [Применить](#) [Сбросить](#)

Рисунок 49. Настройки защищаемого сервера

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.** Значение 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 значения доступно поле *Префикс в URL*. 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) и порт (при необходимости).
- **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 *roundrobin*, 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 отправляется первому доступному серверу.

- *source*. Запросы 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*. Чекбокс доступен после загрузки CA-сертификата и позволяет активировать поле для загрузки сертификата двусторонней аутентификации. Сертификат 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 включенном параметре доступно поле *Временное окно для доступа к ЗР*, поле определяет промежуток времени, в течение которого токен считается действительным. При выключенном чекбоксе *Защита CSRF* доступна настройка:
 - *Cache*. Чекбокс включает кэш 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*. Имитация поддержки активного соединения (keep-alive) с сервером несмотря на то, что на самом деле соединение будет закрыто после отправки ответа.
- *Расширенные настройки*. Чекбокс включает дополнительные параметры и делает доступными настройки:
 - *Тайм-аут сервера*. Устанавливает максимальное время ожидания отправки данных серверу.
 - *Тайм-аут подключений*. Задаёт максимальное время ожидания успешного подключения к серверу.
 - *Тайм-аут состояния*. Задаёт 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 Ресурсы WAF. Если поле *Описание* не заполнено, то будет отображаться *Имя* сервера.

Вкладка **Защищаемые ресурсы** (см. Рисунок 50) 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.

Панель **Домены для инспекции Веб МЭ** позволяет добавлять, изменять и удалять домены для инспекции. Добавление доменов для инспекции может осуществляться с использованием сгенерированного **WAF Dallas Lock** самоподписанного сертификата защищаемого ресурса или готового сертификата сгенерированного сторонним УЦ, подробнее в разделе 5.7.1 Серверные сертификаты.

Для добавления защищаемого ресурса с использованием сгенерированного **WAF Dallas Lock**

самоподписанного сертификата, необходимо в выпадающем списке выбрать сгенерированный сертификат и нажать кнопку **Добавить**. В случае если используется сертификат сгенерированный сторонним УЦ, необходимо нажать кнопку «...», выбрать файл сертификата и нажать кнопку **Загрузить**.

После добавления сертификата откроется страница предварительной настройки защищаемого ресурса.

Ресурсы WAF

Защищаемые серверы Защищаемые ресурсы

Домены для инспекции Веб МЭ

Имя ресурса	Защищаемый сервер	Включено	HTTP	
server.dl.local	server.dl.local	☒	☒	Изменить Удалить

Загрузить новый сертификат

Добавить защищаемый ресурс

Сохранить Применить Сбросить

Рисунок 50. Добавление и редактирование защищаемого ресурса

5.1.2.1 Общие параметры защищаемого ресурса

На вкладке *Общие* можно настроить дополнительные параметры защищаемого ресурса, указав защищаемый сервер, на котором он располагается, а также настроив возможность работы с HTTP-трафиком (если чекбокс *HTTP* выключен, то используется HTTPS соединение). В случае необходимости можно добавить дополнительные сервера для веб-приложения (см. Тип сервера в разделе 5.1.1 Инспекция WAF). Затем необходимо включить защищаемый ресурс в работу WAF Dallas Lock, поставив чекбокс в строке *Включено* (см. Рисунок 51).

Общие Профиль приложения Политика контента Анализ поведения пользователя

Имя ресурса server.dl.local

Включено ☒

Защищаемый сервер server.dl.local

Дополнительные серверы [- пусто -]

HTTP ☒

Отпечаток сертификата bdda75d53c70674db22b31b950fc5eec76c2950ec5905d6c4a390101a63aaa66

Назад Сохранить Применить Сбросить

Рисунок 51. Общие настройки

5.1.2.2 Профиль приложения защищаемого ресурса

Вкладка *Профиль приложения* (см. Рисунок 52) позволяет настроить опции профиля рассматриваемого объекта.



Общие | Профиль приложения | Политика контента | Анализ поведения пользователя

Имя ресурса

server.dl.local

Пресеты

Включить

☒

Пресеты

Пресеты x 3 ^

по умолчанию

Посмотреть правила для этого ресурса

Посмотреть...

Журналирование запросов

Уровень логирования

Все запросы

Контроль адресов запросов

Включить

☐

Допустимая схема URL

...

Политики

Запретить

Настройка журнала

☐

Защита аутентификации

Включить

☐

Точка аутентификации

Количество попыток

5

✓

за 1 мин.

Таймаут

30s

✓

Действие

Заблокировать IP

Защита API

Включить

☐

Тип

XML-RPC

Конечная точка

Загрузить схему

...

Настройка журнала

☐

Содержание политики

Включить

☐

Параметры

Назад

Сохранить

Применить

Сбросить

Рисунок 52. Настройки правил WAF. Защищаемые ресурсы

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 *Включить*.

Пункт **Журналирование запросов** необходим для изменения параметров режима журналирования поступающих запросов на защищаемый ресурс («Все запросы», «Запросы с ошибками»).

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 *Включить*. Функция *Допустимая схема URL* обеспечивает загрузку файла схемы допустимых URL. Параметр *Настройка журнала* необходима для редактирования и настройки выходных данных в журнале.

Использование механизма контроля адресов запросов позволяет разрешить или запретить доступ к определенным страницам или каталогам веб-сайта. Для подготовки файла с допустимой схемой URL необходимо создать текстовый файл, где каждая строка должна начинаться с символа «/» и содержать только один путь (пример: из URL `https://example.com/product/page.php` выделить только `/product/page.php`), в строке должны отсутствовать лишние символы (см. Рисунок 53).



Структура записей в файл позволяет гибко управлять механизмом контроля адресов запросов:

- / — разрешение или ограничение доступа ко всему сайту;
- /path — разрешение или ограничение доступа ко всем страницам в указанном каталоге;
- /path/page1.php — разрешение или ограничение доступа к конкретной странице.

```
*scheme.txt – Блокнот
Файл  Правка  Формат  Вид  Справка
/home
/about
/contact
/product/page1.php
/product/page2.html
```

Рисунок 53. Файл с допустимой схемой URL

Пункт **Защита аутентификации** необходим для настройки авторизации на защищаемом домене. Указываются точка 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*. Включить данный параметр возможно, установив чекбокс напротив *Включить*.



В поле *Точка аутентификации* необходимо указывать путь к странице авторизации, при этом выделять из URL-адреса путь (например: из URL `https://example.com/path/login.php` выделить только `/path/login.php`).

Пункт **Защита API** необходим для выбора схемы вызова процедур, направленных на защиту API клиента. Возможность выбора типа загружаемой схемы: *SOAP*, *XML-RPC*. Для типа схемы *XML-RPC* можно указать значение конечной точки. Функция *Загрузить схему* обеспечивает загрузку внешнего файла схемы веб-приложения в формате «.wsdl» или «.xsd». Параметр *Настройка журнала* необходим для редактирования и настройки выходных данных в журнале. Включить данный параметр возможно, установив чекбокс напротив *Включить*.

Пункт **Содержание политики** необходим для активации политик контента и просмотра настроенных параметров на вкладке *Политики контента*. Активировать политики контента возможно, установив чекбокс напротив *Включить*. Текстовое поле *Параметры* не доступно для редактирования и содержит в себе параметры политик контента в текстовой форме (см. [5.1.2.3 Политики контента защищаемого ресурса](#)).

5.1.2.3 Политики контента защищаемого ресурса

На вкладке *Политика контента* можно определить набор допустимых источников для каждого типа ресурса (см. Рисунок 54).



Общие Профиль приложения Политика контента Анализ поведения пользователя

Имя ресурса	server.dl.local
DEFAULT-SRC	- +
SCRIPT-SRC	- +
STYLE-SRC	- +
IMG-SRC	- +
CONNECT-SRC	- +
FONT-SRC	- +
OBJECT-SRC	- +
MEDIA-SRC	- +
FRAME-SRC	- +
SANDBOX	- +
REPORT-URI	- +
CHILD-SRC	- +
FORM-ACTION	- +
FRAME-ANCESTORS	- +
PLUGIN-TYPES	- +

Назад Сохранить Применить Сбросить

Рисунок 54. Настройки правил WAF. Защищаемые ресурсы

Политика контента защищаемого ресурса (Content Security Policy) — механизм защиты веб-сайтов от атак типа межсайтового скриптинга (XSS) и других угроз, связанных с использованием недоверенных ресурсов. Для настройки доступны следующие политики контента:

- **DEFAULT-SRC** — ограничивает источники для всех типов контента, которые могут быть загружены без конкретной настройки других политик;
- **SCRIPT-SRC** — ограничивает источники для загрузки сценариев;
- **STYLE-SRC** — ограничивает источники для загрузки CSS файлов;
- **IMG-SRC** — ограничивает источники для загрузки изображений;
- **CONNECT-SRC** — определяет с какими доменами возможно создать соединение через AJAX или WebSocket;
- **FONT-SRC** — ограничивает источники для загрузки шрифтов;
- **OBJECT-SRC** — ограничивает источники для загрузки объектов HTML;
- **MEDIA-SRC** — ограничивает источники для мультимедийных файлов;
- **FRAME-SRC** — определяет адреса с которых возможно размещение iframe (элемент HTML, который позволяет встраивать внешний контент внутри текущего документа);
- **SANDBOX** — создает изолированную среду для выполнения кода, позволяющую блокировать потенциально опасные действия;
- **REPORT-URI** — определяет адреса, куда отправляются отчеты о нарушениях CSP;
- **CHILD-SRC** — ограничивает источники контента, используемого для отображения в плагинах или встроенных объектах;
- **FORM-ACTION** — определяет внешние домены, которым разрешено обрабатывать формы;
- **FRAME-ANCESTORS** — определяет внешние домены, которым разрешено содержать текущий сайт в iframe;
- **PLUGIN-TYPES** — определяет типы разрешенных плагинов.

При необходимости для каждой политики контента можно указать несколько значений, для этого необходимо нажать на + и добавить еще одно значение параметра. Каждое значение параметра должно быть указано в отдельном текстовом поле.

Поля политик контента могут содержать следующие записи:

- 'self' — загрузка объектов будет доступна только с текущего защищаемого ресурса;

- домен (пример: example.com) — загрузка объектов будет доступна только для выбранного домена;
- домен и поддомены (пример: *.domain.com) — загрузка объектов будет доступна с выбранного домена и его поддоменов;
- * — загрузка разрешена с любого домена;
- URL (пример: https://example.com/reports) — ссылка на хранилище для хранения отчетов (только для параметра REPORT-URL);
- none — загрузка объектов запрещена с любого домена;
- пустое поле — ограничения не применяются.



Для более гибкой настройки политики контента защищаемого ресурса рекомендуется изучить документацию на Content Security Policy (CSP).

Для завершения процедуры создания защищаемого ресурса необходимо нажать кнопки **Сохранить** и **Применить**.

5.1.2.4 Анализ поведения пользователей

Для настройки анализа поведения пользователей или изменения ранее настроенных параметров защищаемого ресурса необходимо вернуться на вкладку *Защищаемые ресурсы* (Рисунок 55) и нажать кнопку **Изменить** напротив защищаемого ресурса.

Ресурсы WAF

Защищаемые серверы

Защищаемые ресурсы

Домены для инспекции Веб МЭ

Имя ресурса	Защищаемый сервер	Включено	HTTP	
server.dl.local	server.dl.local	☒	☒	Изменить Удалить

Загрузить новый сертификат

...

Загрузить

Добавить защищаемый ресурс

Выберите...

Добавить

Перейти к генерации сертификатов

Сохранить

Применить

Сбросить

Рисунок 55. Добавление и редактирование защищаемого ресурса

На вкладке *Анализ поведения пользователя* (см. Рисунок 56) можно управлять возможностью анализа трафика и блокировки переходов на защищаемом ресурсе при помощи графа связей.

Общие

Профиль приложения

Политика контента

Анализ поведения пользователя

Имя ресурса

server.dl.local

Обучение

Количество переходов:

10000

Процесс обучения:

100.00 % (500 / 500)

Управление обучением:

Старт

Остановить

Очистить

Открыть граф связей

Анализ поведения пользователей

Пороговое значение:

10

Включить

Назад

Рисунок 56. Анализ поведения пользователей



Граф связи и переходов на защищаемом ресурсе основан на теории графов и содержит в себе следующие понятия:

- Граф связей — совокупность данных о защищаемом ресурсе, включающая список узлов и ребер графа, а также общий весовой коэффициент графа связей.
- Узел — URL-ссылка на страницу защищаемого ресурса, представляющая элемент графа.
- Узел-источник — узел (ссылка), с которого пользователь переходит на другую страницу защищаемого ресурса.
- Целевой узел — узел назначения, на который пользователь пытается перейти с узла-источника.
- Ребро графа — связь между двумя узлами графа. Ребро может быть направленным (от узла-источника к целевому узлу) или двусторонним (обозначать прямой и обратный переход между узлами).
- Весовой коэффициент отдельной связи — целочисленное значение, которое отражает количество переходов по ребру, выполненных пользователями во время обучения графа связей.
- Весовой коэффициент графа связей — целочисленное значение, которое устанавливает минимальный порог для весовых коэффициентов ребер в графе. Если вес ребра связи между узлом-источником и целевым узлом ниже этого порога, переход между ними будет заблокирован.

Эти элементы формируют структуру графа, которая используется для анализа трафика и блокировки несанкционированных переходов на защищаемом ресурсе.

Для обучения графа связи необходимо в текстовом поле *Количество переходов* указать объем выборки для обучения и нажать кнопку **Старт**. Затем выполнить следующие действия:

- открыть защищаемый ресурс по доменному имени (например: <https://server.dl.local>);
- выполнить все возможные переходы от узлов-источников к целевым узлам (например: перейти в раздел меню, перейти на страницу авторизации, авторизоваться, обновить страницу).

В процессе обучения будут созданы узлы графа и ребра связи между ними. Для каждого ребра будет установлено количество переходов по маршруту от узла-источника к целевому узлу. Процесс обучения графа связи можно приостановить нажатием кнопки **Остановить**.



При обучении графа связей и переходов необходимо учитывать различные сценарии доступа к узлам (страницам) защищаемого ресурса. Один из важных аспектов — это возможность прямого перехода на узел через ввод URL-адреса в строку поиска браузера или получение доступа через внешние ссылки, такие как поисковая выдача или другой сайт.

Дополнительное обучение графа можно выполнить, нажав кнопку **Старт**, при этом необходимо указать новое значение в поле *Количество переходов* (если ранее было указано количество переходов 5000, то для добавления 500 переходов нужно указать значение 5500). В ходе дополнительного обучения могут быть добавлены новые узлы, новые ребра связи, а также изменены весовые коэффициенты существующих ребер. Для очистки содержимого графа связей можно нажать кнопку **Очистить**.

Поле *Пороговое значение* задает минимальный весовой коэффициент ребра связи, при котором переход считается разрешенным. Кнопка **Включить** активирует анализ трафика и блокировку переходов на защищаемом ресурсе с использованием графа связей. Анализ трафика производится на основе сравнения перехода между узлом-источником и целевым узлом в трафике с параметрами графа связей. Блокировка перехода происходит в следующих случаях:

- если в обученном графе связей отсутствует ребро связи, соответствующее узлу-источнику и целевому узлу;
- для ребра связи, соответствующего узлу-источнику и целевому узлу, установлен параметр «Запретить»;
- если весовой коэффициент ребра связи между узлом-источником и целевым узлом ниже порогового значения весового коэффициента графа связей.



Для активации анализа поведения пользователей требуется изменить конфигурацию некоторых сервисов, что приведет к их перезапуску (см. Рисунок 57).

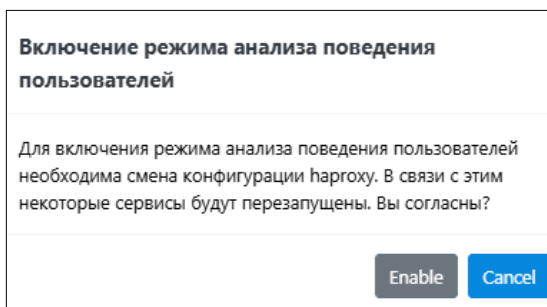


Рисунок 57. Включение режима анализа поведения пользователей

Для отключения анализа трафика и блокировки переходов на защищаемом ресурсе с помощью графа связей нужно нажать кнопку **Отключить**. Для просмотра графа связей и изменения его параметров, следует нажать кнопку **Открыть граф связей**.



Во время обучения графа связи изменение его параметров недоступно.

Страница изменения параметров графа связей содержит в себе панель отображения графа связей и панель инструментов.

Страница отображения графа связей и переходов на защищаемом ресурсе состоит из двух панелей: *Панель отображения графа связей* и *Панель настроек*.

На панели отображения графа связей находятся следующие элементы:

- поле поиска, предназначенное для поиска узлов графа;
- элементы управления масштабированием: увеличение, уменьшение масштаба и центрирование графа связей;
- шкала выбора минимального значения весового коэффициента ребра связи, при котором на панели отображения подсвечиваются ребра связи с коэффициентами выше установленного;
- граф связей, где узлы изображены точками, а связи между ними — кривыми линиями.



При отображении графа связей выделяются следующие элементы:

- зеленая точка — узел, соответствующий доменному имени защищаемого ресурса;
- оранжевая точка — узел «empty-referrer», при обучении графа связи доступ к целевому узлу был получен напрямую, в адресную строку был введен адрес страницы сайта или переход был осуществлен с постороннего ресурса;
- ребро связи черного цвета — в параметрах графа связей для данного ребра установлен параметр «Запретить»;
- при выборе узла или ребра связи отображаются весовые коэффициенты всех ребер связи, связанных с элементом графа.

Панель настроек предоставляет информацию и позволяет изменять параметры для выбранных элементов графа:

- При выборе узла становятся доступны следующие разделы:
 - *Настройки узла*, в котором отображаются количество ребер связи для данного узла;
 - *Связи узла*, в котором отображаются связи выбранного узла с другими узлами, представленные в виде записи «(количество переходов) узел-источник → целевой узел», а также чекбокс, позволяющий запретить переход по соответствующему ребру связи.
- При выборе ребра связи на панели инструментов становится доступен раздел *Переход*, в котором отображается запись вида «(количество переходов по ребру) узел-источник → целевой узел», а также чекбокс, позволяющий запретить переход по ребру связи.

При изменении параметров на панели отображаются раздел *Внесенные изменения*, где отображаются все внесенные изменения и кнопки **Сохранить** и **Очистить**, которые позволяют сохранить или отменить внесенные изменения соответственно.

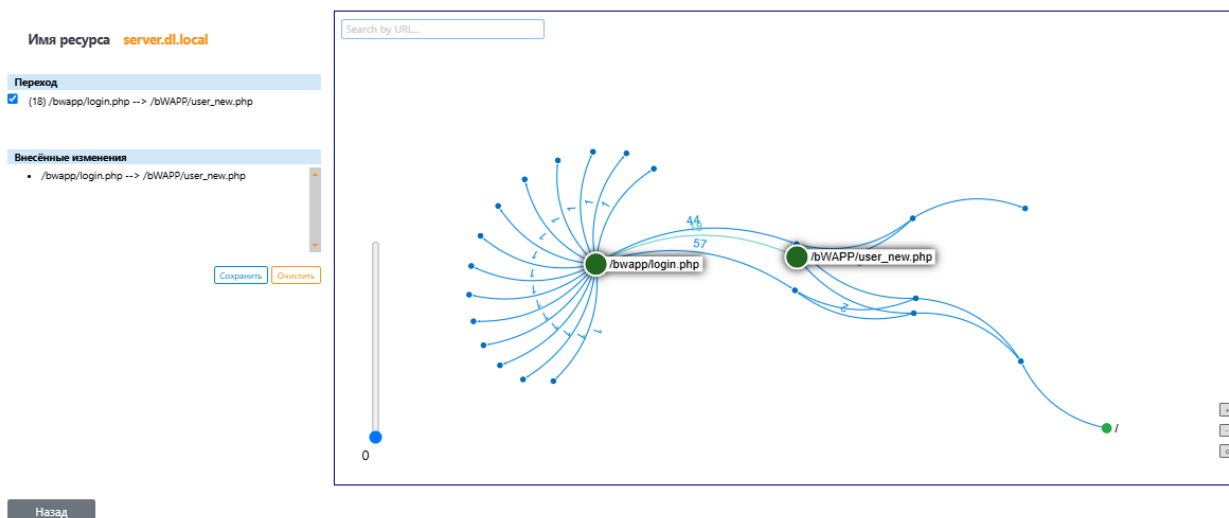


Рисунок 58. Параметры графа связей

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. Все узлы делятся на два типа: *VRRP Master* и *VRRP Backup*. В каждый момент времени только устройство с ролью *Master* обрабатывает весь трафик, связанный с защищаемыми ресурсами.

Необходимо в **Настройках** перейти в раздел **WAF** и выбрать пункт *Настройка кластеризации* (см. Рисунок 59).

! Механизм кластеризации не берет на себя функцию «балансировщика» трафика. *Backup* устройства синхронизируются с *Master* устройством для обновления данных, на которое приходится вся нагрузка сети. *Backup* устройство предназначено для подмены основного в случае, если оно выйдет из строя.

Настройки ^	Сеть v	Перезагрузка
WAF >	Инспекция WAF >	
UTM >	Ресурсы WAF >	
Настройки модуля ЕЦУ	<u>Настройка кластеризации</u>	
Общие >	Фильтр содержимого	

Рисунок 59. Пункт Настройка кластеризации в меню

Чтобы создать новый кластер, необходимо установить галочку в соответствующем чекбоксе (см. Рисунок 60), после чего для редактирования будут доступны два блока:

- **Настройки виртуального интерфейса для WAF**, где необходимо выбрать интерфейс и задать виртуальный IP для него.
- **Настройки виртуального интерфейса для репликаций**, где необходимо выбрать интерфейс и задать виртуальный IP для него.



Для блока **Настройки виртуального интерфейса для WAF** или **Настройки виртуального интерфейса для репликаций** в поле *Интерфейс* могут быть выбраны только интерфейсы, для которых не установлен или установлен чекбокс *Доверенный интерфейс* соответственно, подробнее в разделе [6.1 Интерфейсы](#).

Общие настройки

Создать кластер	☒
Войти в кластер	Перейти к отключению WAF
Статус	MASTER

Настройки виртуального интерфейса для WAF

Интерфейс	WAN
Виртуальный IP	192.168.23.199/32

Настройки виртуального интерфейса для репликаций

Интерфейс	LAN
Виртуальный IP	192.168.1.250/24

Сохранить

Применить

Сбросить

Рисунок 60. 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 61). Здесь же через нажатие соответствующих кнопок можно вывести узел из кластера или сделать резервное устройство *Master-устройством*.

Список узлов

Статус	Имя узла/IP	Последнее соединение, сек. назад	Приоритет		
BACKUP	Текущий узел		254		
MASTER	sword.222/192.168.40.222	10	255	Вывести из кластера	Сделать Мастером
BACKUP	sword.223/192.168.40.223	260936	109	Вывести из кластера	Сделать Мастером

Рисунок 61. Список узлов

Чтобы войти в уже существующий кластер, необходимо нажать на ссылку *Перейти к отключению WAF* и включить инспекцию WAF на открывшейся странице (см. Рисунок 60).

После отключения инспекции WAF появится чекбокс «Войти в кластер» (см. Рисунок 62), после чего появится окно выбора конфигурационных настроек.

Общие настройки

Войти в кластер	☒
Создать кластер	Перейти к включению WAF
Включить этот узел в WAF-кластер	... Загрузка

Сохранить

Применить

Сбросить

Рисунок 62. Добавление узла в кластер

В случае, если *Master* выходит из строя, его подменяет одно из резервных устройств, которому переходит статус *Master*. Новый *Master* способен прозрачно подхватить и продолжить обработку

сетевых потоков. Если в **Общих настройках** включен режим вытеснения (см. Рисунок 63), изначальный *Master* возвращает себе все права, как только его работа возобновляется.

Общие настройки

Текущий статус	BACKUP/Запущен
Скачать конфигурацию	Скачать конфигурацию
Выйти из кластера	Выйти из кластера
Приоритет	101
Режим вытеснения	Yes

Рисунок 63. Режим вытеснения

При подключении резервного *Backup* устройства к основному *Master* происходит репликация следующих конфигурационных настроек:

- Пользователи (в том числе заблокированные пользователи);
- Журналы аудита (события из журнала Инциденты);
- Сертификаты (серверные сертификаты, сертификаты УЦ);
- WAF (основные настройки, защищаемые серверы, клиенты (аутентификация по CA), защищаемые ресурсы, новые и включенные правила в фильтре содержимого, параметры графа связей и переходов на защищаемом ресурсе);
- Защищаемые серверы (Инспекция WAF);
- UTM (параметры настройки SSL/TLS, новые и включенные правила в фильтре содержимого);
- DHCP & DNS (основные настройки, дополнительные настройки);
- Межсетевой экран (основные настройки, перенаправление портов, правила для трафика, правила аудита трафика, списки доступа);
- Параметры аудитора (параметры настройки журнала, основные, авторизации, фильтра содержимого);
- Качество обслуживания (QOS);
- Статические маршруты (IPv4 & IPv6).

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 64).

Фильтр содержимого

WAF
Пресеты
Обновить
Настройка config файла

☐ Активировать правила WAF
77 / 9286 / 9275
активно / настроено / БРП

Пресет
Имя ресурса
IP
Фильтр правил...
Фильтр
Выводить по: 10
☐ Только включенные
Сбросить фильтры
9 / 18 / 10

Выбрать правила...
Отметить как просмотренные

☐	Angular Magecart попытка JS инъекции [0900]	Angular JS
☐	Angular Magecart попытка JS инъекции [0901]	Angular JS
☒	Ruby in Rails Попытка SQL инъекции [0903]	Инъекции
☒	MySQL ошибка в HTTP ответе, возможно SQL инъекция [0904]	Инъекции
☒	MySQL ошибка в HTTP ответе, возможно SQL инъекция [0905]	Инъекции
☒	MySQL ошибка в HTTP ответе, возможно SQL инъекция [0906]	Инъекции
☒	MySQL ошибка в HTTP ответе, возможно SQL инъекция [0907]	Инъекции
☒	MySQL ошибка в HTTP ответе, возможно SQL инъекция [0908]	Инъекции
☒	MySQL ошибка в HTTP ответе, возможно SQL инъекция [0909]	Инъекции
☒	Обнаружен сканер SQL инъекций [0910]	Инъекции

Рисунок 64. Настройка правил WAF. Фильтр содержимого. WAF

Для включения или отключения нескольких правил одновременно следует нажать кнопку **Выбрать правила**, выбрать нужные правила и нажать соответствующую кнопку.

WAF управляет сетевым трафиком к веб-серверам, расположенным в DMZ зоне, основываясь на наборах правил, которые определяют, как обрабатывать входящие и исходящие пакеты данных. В зависимости от параметров правила WAF, возможны следующие действия с трафиком:

- Отвергнуть (reject). Трафик блокируется, но отправителю сообщается, что его пакет не был доставлен.
- Заблокировать (block). Трафик блокируется без уведомления отправителя.
- Пропустить (pass). Трафик разрешается и проходит через межсетевой экран.
- Тревога (alert). Трафик разрешается, но при этом фиксируется в журнале для последующего анализа.

Для удобства администрирования межсетевого экрана уровня веб-сервера правила объединены в отдельные категории (пресеты). Пресеты содержат в себе правила обработки сетевого трафика.

Существует возможность изменить правила под свою инфраструктуру, задав уточняющие данные, либо включить/отключить составляющие политики для правила (см. Рисунок 65).

!

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

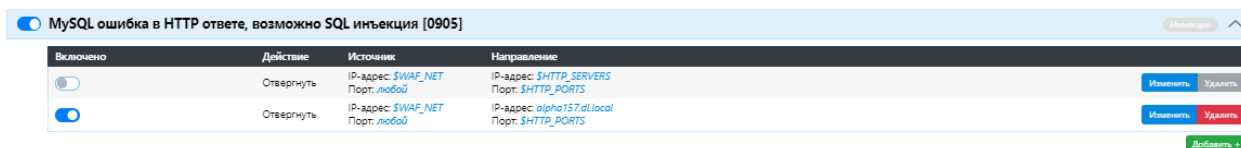


Рисунок 65. Настройка правила WAF. Фильтр содержимого. WAF

Страница изменения и просмотра правила WAF (Рисунок 66) может содержать следующие поля:

- ID/Ревизия — уникальный идентификатор правила и номер ревизии правила, используемый для отслеживания изменений.
- Пресет (приложение) — пресет, к которому относится правило.
- Тип OWASP10 — тип атаки или уязвимости согласно OWASP Top 10.
- Тип события безопасности — краткое описание атаки или уязвимости.
- Уровень атаки — относительная важность срабатывания определенного правила: высокий, средний, низкий.
- Тип трафика — классификации передаваемых данных, в зависимости от используемого приложения или протокола.
- Протокол нижнего уровня — протокол транспортного, сетевого или канального уровня.
- Действие (см. выше).
- Источник.
- Порт источника.
- Направление.
- Порт направления.
- Направление и/или состояние трафика — направление и/или состояние сетевого трафика, к которому должно применяться правило.
- Дополнительные параметры пакета — параметры для более точного определения и классификации сетевых пакетов.
- Правила контекстного фильтра — условия, при которых правило срабатывает на основе содержимого, например, поиск определенных строк или байтов внутри пакета.

WAF Пресеты Обновить Настройка config файла

SERVER-OTHER PHP 4 unserialize ZVAL Reference Counter Overflow attempt [базовое правило]

Включено

ID / Ревизия 31055 / 3

Пресет (приложение) SERVER-OTHER

Тип события безопасности Попытка получения привилегий администратора

Уровень атаки Средний [2]

Тип трафика HTTP

Протокол нижнего уровня TCP

Действие Отвергнуть [reject]

Источник \$WAF_NET

Порт источника Любой

Направление \$HTTP_SERVERS

Порт назначения \$HTTP_PORTS

Направление и/или состояние трафика to_server,established

Дополнительные параметры пакета 'dsize' : '>4800'

Правила контекстного фильтра

```
[
  {
    "content": {
      "string": "cookie:"
    }
  },
  {
    "isdateat": "3600,relative"
  },
  {
    "content": "[\\"|@0 0A|\\""
```

Назад Применить Сбросить

Рисунок 66. Настройка правил WAF. Фильтр содержимого. WAF

Поле *Дополнительные параметры пакета* может содержать одно или несколько из перечисленных ниже значений (см. Таблица 3). Если в правиле информация в этом поле отсутствует, оно будет скрыто.

Таблица 3. Перечень атрибутов поля «Дополнительные параметры пакета»

Наименование	Назначение	Атрибуты
ack	Проверка номеров подтверждения TCP	-
dsize	Проверка размера поля данных пакета	-
flags	Проверка наличия заданных флагов TCP	-
flowbits	Проверка правил для сеансов транспортного уровня	-
fragbits	Проверка наличия в заголовке IP битов фрагментации и резервного бита	M — проверять бит фрагментации; D — проверять бит запрета фрагментации; R — проверять резервный бит
fragoffset	Сравнение смещения фрагмента дейтаграммы IP с заданным десятичным значением	-
icmp_id	Проверка значений идентификаторов ICMP	-
icmp_seq	Проверка порядковых номеров ICMP	-
icode	Проверка значения кода ICMP	-
id	Проверка наличия в поле IP ID заданного значения	-
ip_proto	Проверка идентификатора протокола в заголовке IP	-
ipopts	Проверка наличия в заголовке IP опций	rr — запись маршрута; eol — завершение списка опций;

		nor — нет опций; ts — временная метка; sec — опция безопасности; lsrr — не жестко заданный отправителем маршрут; ssrr — жестко заданный отправителем маршрут; satid — идентификатор потока; any — любые опции
itype	Проверка типа сообщения ICMP	-
sameip	Обнаружение пакетов с совпадающими адресами IP для источника и направления	-
seq	Проверка значений порядковых номеров TCP	-
stream_size	Проверка размера потока TCP	-
tos	Проверка в пакетах поля IP TOS (тип обслуживания)	-
ttl	Проверка времени жизни дейтаграмм IP	-
window	Проверка размера окна TCP	-

Поле *Правила контекстного фильтра* может содержать одно или несколько из перечисленных ниже ключевых слов (см. Таблица 4). Если в правиле информация в этом поле отсутствует, оно будет скрыто.

Таблица 4. Перечень атрибутов поля «Правила контекстного фильтра»

Наименование	Назначение
content	Позволяет искать определенное содержимое в полезной нагрузке пакета и запускают ответ на основе этих данных
depth	Задаёт, сколько байтов от начала данных пакета следует просматривать для поиска сопоставления. Например, если указано depth: 5, WAF будет искать только в первых пяти байтах от заданной позиции
distance	Определяет, сколько байтов следует пропустить после последнего сопоставляемого содержимого перед началом следующего поиска. Его часто используют после content для указания, где начинать новый поиск
offset	Задаёт количество байтов с начала полезной нагрузки пакета, с которого должен начаться поиск контента. Указывает начальную точку поиска
within	Определяет максимальное количество байтов, в пределах которого нужно найти следующее сопоставление после исходного поиска. Используется для указания допустимого диапазона для поиска
nocase	Задаёт, что поиск контента должен быть нечувствителен к регистру. Полезен для поиска текстовых данных, где регистр неважен
rawbytes	Указывает, что поиск будет происходить в необработанных байтах пакета, без участия каких-либо декодеров или препроцессоров, которые могли бы изменить данные
http_client_body	Проверяет содержимое тела HTTP-запроса, отправляемого клиентом на сервер. Это позволяет искать вложения или другие типы данных, которые передаются как часть тела запроса
http_cookie	Осуществляет проверку значений, содержащихся в заголовках HTTP Cookie

http_raw_cookie	Анализирует необработанную строку Cookie, как она была прислана, что полезно для выявления атак с использованием закодированных или каким-либо образом измененных данных Cookie
http_header	Анализирует все HTTP-заголовки в запросе или ответе. Это важно для изучения специфических или аномальных заголовков
http_raw_header	Проводит проверку всех необработанных HTTP-заголовков, полезно для анализа переданных строк в их оригинальной форме
http_method	Анализирует метод HTTP-запроса, такой как GET, POST, PUT и другие
http_uri	Проводит анализ и проверку части URI запроса, используемой клиентом. Этот модификатор позволяет фокусироваться на анализе маршрутов и параметров в URI
http_raw_uri	Осуществляет проверку полной необработанной строки URI в запросе
http_stat_code	Осуществляет проверку кода состояния HTTP-ответа, например, 200, 404 и т.д.
http_stat_msg	Анализирует текстовое сообщение состояния HTTP-ответа, объясняющее код состояния
fast_pattern	Используется для улучшения производительности сопоставления, определяя часть содержимого как «быстрый шаблон», который помогает эффективнее выполнять массовый поиск сопоставлений. Это достигается оптимизацией начального поиска, чтобы быстро исключить несоответствующие пакеты
file_data	Используется для указания на обработку содержимого файлов (file inspection) в контексте сетевых пакетов
uricontent	Выполняет поиск в нормализованном поле URI запроса
isdataat	Проверяет, присутствует ли указанное количество данных в пределах полезной нагрузки или следуют ли какие-либо фрагменты
pcre	Использует регулярные выражения Perl Compatible для сложного поиска в полезной нагрузке
byte_test	Позволяет проводить побитовые и числовые тесты на указанных байтах полезной нагрузки
byte_jump	Используется для перескакивания определенного количества байтов (на основе значения), найденного в полезной нагрузке, что полезно для парсинга протоколов с динамической длиной
byte_extract	Используется для извлечения целочисленных значений из полезной нагрузки пакета

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 67).

Фильтр содержимого ⓘ

WAF Пресеты Обновить Настройка config файла

Пользовательские пресеты

Название пресета	Тестовый пресет ✓ 0 правил(о,а)	Удалить секцию
Защищаемые ресурсы	server.dl.local ✓ +	

Добавить +

Пресеты

Название пресета	WEB Scanner ✓ 11 правил(о,а)	Удалить секцию
Защищаемые ресурсы	server.dl.local ✓ +	

Название пресета	Базовый Веб МЭ ✓ 13 правил(о,а)	Удалить секцию
Защищаемые ресурсы	server.dl.local ✓ +	

Angular.js [2] + Добавить +

Сохранить

Применить

Сбросить ▾

Рисунок 67. Настройка правил WAF. Фильтр содержимого. Пресеты

Предустановленные пресеты межсетевого экрана уровня веб-сервера предназначены для защиты веб-приложений от различных видов атак (см. Таблица 5).

Таблица 5. Пресеты WAF

Наименование пресета	Назначение
! Angular.js	защита веб-серверов, использующих фреймворк Angular.js
! Apache	защита веб-серверов Apache
! Bitrix	защита веб-серверов, использующих систему управления контентом Bitrix
! Forbidden Data	обнаружение трафика, содержащего текстовый контент определенных кодировок и нетекстовый контент
! Forbidden Methods	обнаружение трафика, содержащего методы HTTP
! JQuery	защита веб-серверов, использующих библиотеку JavaScript JQuery
! Scanner Dir-Traversal	обнаружение трафика, генерируемого при сканировании веб-уязвимостей связанных с обходом директорий
! Scanner Injections	обнаружение трафика, генерируемого при сканировании веб-уязвимостей связанных с инъекциями
! Scanner other	обнаружение трафика, генерируемого при сканировании иных веб-уязвимостей
! Scanner RCE	обнаружение трафика, генерируемого при сканировании веб-уязвимостей, направленных на удаленное выполнение кода
! Scanner XSS	обнаружение трафика, генерируемого при сканировании веб-уязвимостей, направленных на внедрение вредоносных скриптов в веб-страницы
! WEB Scanner	обнаружение трафика, генерируемого инструментами для сканирования веб-уязвимостей
! WordPress	защита веб-серверов, использующих систему управления контентом WordPress
! Базовый Веб МЭ	защита веб-серверов
! Инъекции	защита веб-серверов от SQL-инъекций, внедрения команд операционной системы и иных видов инъекций

Наименование пресета	Назначение
APP-DETECT	обнаружение трафика, генерируемого определенными приложениями, работающими в сети
BROWSER-IE	обнаружение трафика, содержащего попытки использования уязвимостей или особенностей работы браузера Internet Explorer
BROWSER-OTHER	обнаружение трафика, содержащего попытки использования уязвимостей или особенностей работы браузеров (в основном Opera)
EXPLOIT-KIT	обнаружение трафика, с использованием сигнатур известных эксплоитов
FILE-FLASH	обнаружение подозрительного трафика к Adobe Flash Player
FILE-IDENTIFY	обнаружение файлов с определенным идентификатором в трафике
FILE-IMAGE	обнаружение трафика, нацеленного на эксплуатацию уязвимостей в файлах изображений
FILE-JAVA	обнаружение трафика, нацеленного на эксплуатацию уязвимостей в Java-файлах
FILE-OFFICE	обнаружение трафика, нацеленного на эксплуатацию уязвимостей в файлах офисных программ
FILE-OTHER	обнаружение трафика, нацеленного на эксплуатацию уязвимостей в файлах
FILE-PDF	обнаружение трафика, нацеленного на эксплуатацию уязвимостей в PDF-файлах
INDICATOR-COMPROMISE	обнаружение трафика, содержащего опасные запросы к удаленным ресурсам
INDICATOR-OBfuscATION	обнаружение обфусцированного JS кода в трафике
INDICATOR-SCAN	обнаружение трафика, содержащего попытки сканирования сети
INDICATOR-SHELLCODE	обнаружение трафика, содержащего в пакетах фрагмент машинного кода
MALWARE-BACKDOOR	обнаружение трафика, содержащего запрос соединения с удаленным компьютером, инициализированный вредоносным ПО
MALWARE-CNC	обнаружение трафика от центра управления множеством компьютеров
MALWARE-OTHER	обнаружение трафика, связанного с работой вредоносного ПО, не подпадающего под описание предыдущих двух пунктов
MALWARE-TOOLS	обнаружение трафика, связанного с работой хакерского инструментария
OS-MOBILE	обнаружение трафика, эксплуатирующего уязвимости мобильных операционных систем
OS-OTHER	обнаружение трафика, эксплуатирующего уязвимости операционных систем
OS-WINDOWS	обнаружение трафика, эксплуатирующего уязвимости операционных систем семейства Windows и их компонентов
POLICY-MULTIMEDIA	обнаружение трафика к мультимедийным ресурсам
POLICY-OTHER	обнаружение трафика к определенным ресурсам
POLICY-SOCIAL	обнаружение трафика к социальным сетям
PROTOCOL-OTHER	обнаружение ошибок и потенциальных атак на некоторые протоколы
PROTOCOL-RPC	обнаружение ошибок и потенциальных атак на службы удаленного вызова процедур
PROTOCOL-SCADA	обнаружение ошибок и потенциальных атак на SCADA-системы
PROTOCOL-VOIP	обнаружение ошибок и потенциальных атак на средства голосового общения по сети
PUA-ADWARE	идентификация потенциально нежелательных приложений, связанных с размещением рекламы
PUA-OTHER	идентификация потенциально нежелательных приложений

Наименование пресета	Назначение
PUA-P2P	идентификация потенциально нежелательных приложений, которые используют пиринговые сети (P2P) для обмена файлами (например, торрент-трекеров)
PUA-TOOLBARS	идентификация потенциально нежелательных приложений, таких как нежелательные панели инструментов в веб-браузерах
SERVER-APACHE Apache Struts	обнаружение трафика, эксплуатирующего уязвимости фреймворка Apache Struts
SERVER-APACHE Apache Tomcat	обнаружение трафика, эксплуатирующего уязвимости веб-серверов Apache Tomcat
SERVER-IIS	обнаружение трафика, эксплуатирующего уязвимости веб-серверов IIS
SERVER-IIS Microsoft IIS	обнаружение трафика, эксплуатирующего уязвимости веб-серверов Microsoft IIS
SERVER-MAIL	обнаружение трафика, эксплуатирующего уязвимости почтовых серверов организации
SERVER-MSSQL	обнаружение трафика, эксплуатирующего уязвимости сервера баз данных под управлением MSSQL
SERVER-MYSQL	обнаружение трафика, эксплуатирующего уязвимости сервера баз данных под управлением MySQL
SERVER-ORACLE	обнаружение трафика, эксплуатирующего уязвимости сервера баз данных под управлением Oracle
SERVER-OTHER	обнаружение трафика, эксплуатирующего уязвимости веб-приложений
SERVER-WEBAPP	защита популярных веб-приложений от атак, связанных с эксплуатацией уязвимостей
SERVER-WEBAPP Microsoft Outlook	защита веб-приложения Microsoft Outlook от атак, связанных с эксплуатацией уязвимостей
SQL	защита веб-серверов от SQL-инъекций



Включение большого количества пресетов может существенно увеличить нагрузку на межсетевую экран, что может привести к замедлению обработки трафика веб-сервера. Это связано с тем, что каждый пресет добавляет дополнительную логику и проверки, которые необходимо выполнить. Поэтому важно активировать только те пресеты, которые действительно необходимы для данной инфраструктуры и используемых технологий.

Кроме предустановленных пресетов можно создавать и собственные. Для этого доступны следующие способы создания пресетов:

1. Создать пресет на вкладке *Пресеты*:
 - Нажать кнопку **Добавить** в блоке *Пользовательские пресеты*.
 - Ввести имя пресета и указать защищаемый сервер, используя кнопки **+** или **–** для изменения количества защищаемых серверов.
 - Перейти на вкладку *WAF* и нажать кнопку **Выбрать правила**.
 - Выбрать нужные правила.
 - Нажать кнопку **Добавить в пресет**.
 - Выбрать ранее созданный пресет.
 - Нажать кнопку **Добавить**, чтобы добавить правила в пресет.
2. Создать пресет на вкладке *WAF*:
 - Нажать кнопку **Выбрать правила**.
 - Выбрать нужные правила.
 - Нажать кнопку **Добавить в пресет**.
 - Для создания нового пресета в поле *Пресеты* выбрать *Новый пресет*, ввести его имя и указать защищаемый сервер, используя кнопки **+** или **–** для изменения количества защищаемых серверов (см. Рисунок 68).
 - Нажать кнопку **Добавить**, чтобы правила были добавлены в новый пресет, который

отобразится на вкладке *Пресеты*.

Рисунок 68. Добавление пресета

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 69).



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 правил и их применения к защищаемым ресурсам и отдельным узлам сети.

Фильтр содержимого ⓘ



WAF Пресеты Обновить **Настройка config файла**

По сети Интернет

URL	https://updates.dallaslock.ru/WafUpdate/waf-brp-current.tar.gz
Обновить данные	Обновить
Регулярно по расписанию ⓘ	☐

Из файла

Загрузить		...
-----------	----------------------	------------------------------------

Рисунок 69. Настройка правил WAF. Фильтр содержимого. Обновить

Вкладка *Настройка config-файла* необходима для ручного описания файла конфигурации правил для **WAF** (см. Рисунок 70).

Фильтр содержимого

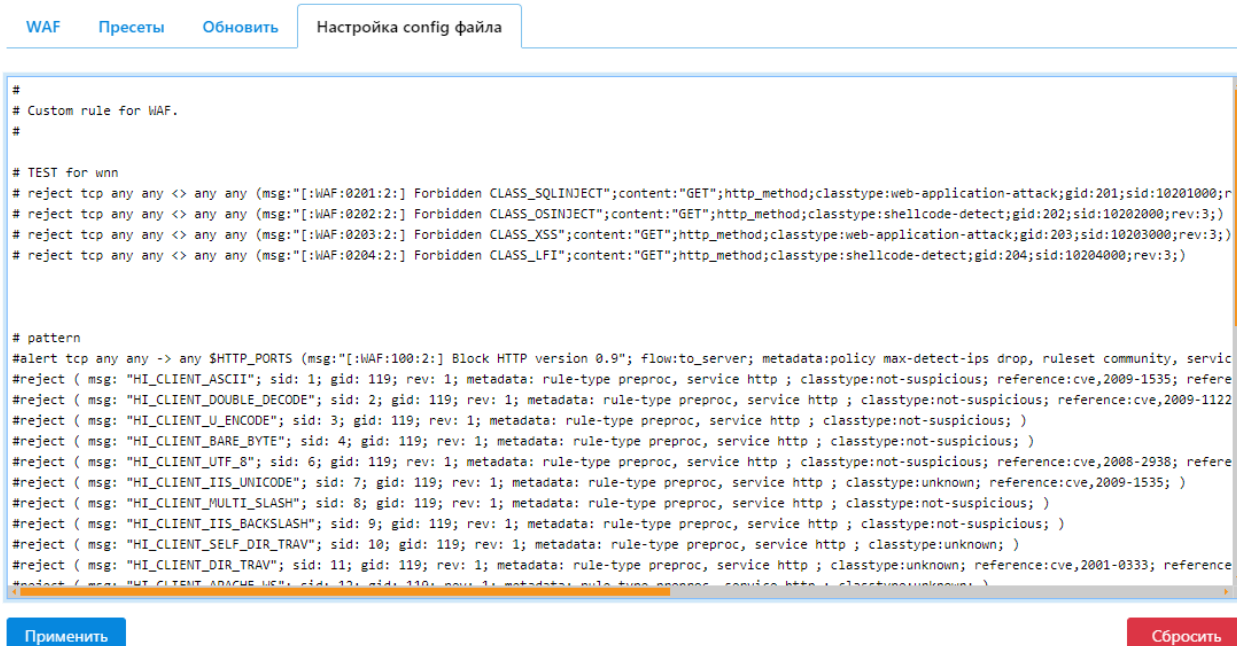


Рисунок 70. Настройка правил WAF. Фильтр содержимого. Настройка config-файла

5.1.5 Настройка инспекции защищаемого узла.

Ниже приведен общий алгоритм загрузки клиентского сертификата для inspectируемого узла.

- Открыть веб-интерфейс управления **WAF Dallas Lock**. В разделе **Настройки** выбрать пункт **WAF — Инспекция WAF — Клиенты**, активировать опцию **Включить аутентификацию по CA**, после чего загрузить CA из файла или по URL (список отзывов сертификатов не является обязательной опцией) и нажать кнопку **Применить**.
- Далее на панели ниже нажать кнопку **Добавить**, затем кнопку «...» и загрузить клиентский сертификат. Нажать кнопку **Применить**.
- Перейти к списку **Защищаемые ресурсы**. На панели загрузки новых сертификатов нажать кнопку выбора файла и загрузить сертификат, в новом окне нажать кнопку **Добавить**.
- В новом окне в пункте **Защищаемый сервер** выбрать inspectируемый узел, если он не был выбран автоматически.
- Если все было сделано корректно, то в списке защищаемых ресурсов появится inspectируемый узел. Также 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 71). Произойдет открытие списка меню третьего уровня.

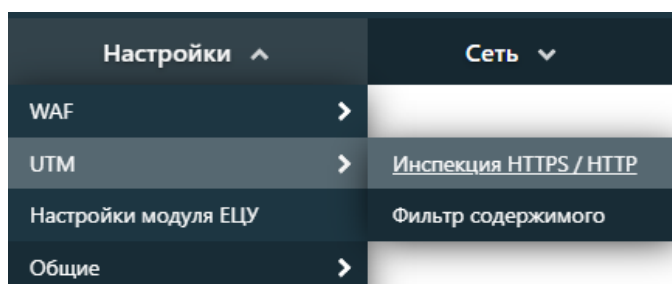


Рисунок 71. Настройка UTM

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 включить чекбокс в разделе *Инспекция HTTPS/HTTP* (см. Рисунок 72).

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 72. Добавление HTTPS/HTTP-сертификата

5.2.2 Фильтр содержимого

Страница *Фильтр содержимого* позволяет настроить основные параметры UTM, COB и МЭ уровня логических границ сети, настроить параметры защиты от несигнатурных угроз и обновить БРП. Страница содержит следующие вкладки:

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

На вкладке *Опции* (см. Рисунок 73) приведена информация о состоянии COB 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 COB. В соответствующих полях указываются такие параметры, как количество срабатываний сигнатур COB и период (в секундах), за который это происходит.

Опции
Несигнатурные угрозы
COB
МЭ
Пресеты
Обновить
Настройка config файла

Статус

COB: 0 / 14992 / 14992
МЭ: 0 / 22 / 22

активно / настроено / БРП

Проверка правил

Проверить

Настройки уведомления о срабатывании сигнатур COB

Количество срабатываний

1

✓

за период

60

✓ сек

Сохранить

Применить

Сбросить

Рисунок 73. Опции

Вкладка *Несигнатурные угрозы* состоит из следующих подвкладок:

- *Фрагментация*;
- *Сканирование портов*;
- *Эвристика*.

На вкладке *Фрагментация* (см. Рисунок 74) 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 — фрагменты IP-пакета содержат несовместимые опции;
- Атака TearDrop — в IP-пакете используются некорректные фрагменты или некорректные смещения;
- Короткие фрагменты (возможность DOS) — IP-пакет фрагментирован на большое число фрагментов;
- Фрагмент продолжается за размер пакета — фрагмент IP-пакета указывает на размер больше размера IP-пакета;
- Фрагмент нулевого размера — фрагмент IP-пакета имеет нулевой размер;
- Фрагмент негативного размера — фрагмент IP-пакета имеет некорректный размер;
- Невозможно большой фрагмент — фрагмент IP-пакета имеет размер, превышающий максимально допустимый;
- Перекрытие фрагментов — фрагменты IP-пакета перекрывают друг друга;
- Атака на BSD с переполнением буфера — специально сконструированные фрагменты IP-пакета используются для переполнения буфера в системах BSD;
- Атака на BSD с лишними фрагментами — отправляются лишние фрагменты IP-пакета для переполнения буфера в системах BSD;
- TTL фрагмента ниже установленного — время жизни фрагмента IP-пакета истекает прежде, чем достигнет получателя (необходимо установить значение для параметра *Минимальный TTL*);
- Перекрытие фрагментов выше установленного — перекрывающиеся фрагменты IP-пакета превышают максимальный размер общих частей между фрагментами (необходимо установить значение для параметра *Перекрытие*);
- Фрагменты меньше установленного минимума — фрагмент IP-пакета имеет размер, менее минимально допустимого (необходимо установить значение для параметра *Размер*).

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).



Атаки с использованием фрагментации направлены на использование особенностей обработки фрагментированных IP-пакетов сетевыми устройствами и могут привести к сбоям или исчерпанию ресурсов получателя при попытках обработать некорректные фрагменты.

Опции
Несигнатурные угрозы
COB
МЭ
Пресеты
Обновить
Настройка config файла

Фрагментация
Сканирование портов
Эвристика

Фрагментация

Таймаут	60	✓
Минимальный TTL	60	✓
Перекрытие	0	✓
Размер	0	✓

Действия при нарушениях фрагментации

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

Рисунок 74. Несигнатурные угрозы — Фрагментация

На вкладке *Сканирование портов* (см. Рисунок 75) настраиваются действия при сканировании портов. **WAF Dallas Lock** позволяет обнаружить события сканирования портов и отслеживать попытки подключения по протоколам TCP, UDP, ICMP и IP:

- Сканирование одним узлом нескольких портов (протоколов) целевого устройства:
 - TCP Portscan;
 - UDP Portscan;
 - IP Protocol Scan;
- Сканирование одним узлом нескольких портов (протоколов) целевого устройства с использованием поддельных IP-адресов:
 - TCP Decoy Portscan;
 - UDP Decoy Portscan;
 - IP Decoy Protocol Scan;
- Одновременное сканирование несколькими узлами нескольких портов (протоколов) целевого устройства:
 - TCP Distributed Portscan;
 - UDP Distributed Portscan;
 - IP Distributed Protocol Scan;

- Сканирование одним узлом нескольких портов (протоколов) нескольких целевых устройств:
 - TCP Portsweep;
 - UDP Portsweep;
 - IP Protocol Sweep;
 - ICMP Sweep;
- Сканирование портов аналогично сценариям, указанным выше, при котором рассматриваются ответы о состоянии портов со значением «Filtered»:
 - TCP Filtered Portscan;
 - TCP Filtered Decoy Portscan;
 - TCP Filtered Portsweep;
 - TCP Filtered Distributed Portscan;
 - IP Filtered Protocol Scan;
 - IP Filtered Decoy Protocol Scan;
 - IP Filtered Protocol Sweep;
 - IP Filtered Distributed Protocol Scan;
 - UDP Filtered Portscan;
 - UDP Filtered Decoy Portscan;
 - UDP Filtered Portsweep;
 - UDP Filtered Distributed Portscan;
 - ICMP Filtered Sweep;
- Сканирование открытых портов целевого устройства — Open Port.

Для события «Open Port» отслеживаются ответы о состоянии портов со значением — «Открыт», для событий «Filtered» — «Отфильтрован», для остальных событий — «Закрыт».

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).

Фрагментация Сканирование портов Эвристика

Сканирование портов

Обнаружение аномалий



Действия при сканировании портов

TCP Portscan	оповестить (alert)
TCP Decoy Portscan	оповестить (alert)
TCP Portsweep	оповестить (alert)
TCP Distributed Portscan	оповестить (alert)

Рисунок 75. 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 76). Для настройки *Уровня эвристического анализа* необходимо перейти в раздел **Настройки — Общие — Настройки — Фильтр содержимого** (более подробно в пункте [5.4.5.2 Настройки переменных фильтра содержимого](#)).

Настройка количества обслуживающих процессов ⓘ

Активный (inline) режим	☒
Экземпляры	2 ✓
Пассивный режим	☒
Интерфейсы	eth1 - +
Инспекция WAF ⓘ	2 ✓

Настройки переменных фильтра содержимого

Внутренние сети ⓘ	172.16.157.0/24,192.168.157.0/24 ✓
DNS-серверы	192.168.13.89,192.168.13.162,\$HOME_NET ✓
Веб-серверы	172.16.157.10
SMTP-серверы	\$HOME_NET ✓
Внешние сети	!\$HOME_NET ✓
SQL-серверы	\$HOME_NET ✓
Внешние сети WAF	!\$HTTP_SERVERS ✓
Уровень эвристического анализа	Низкий
SSL-порты	Средний ✓
HTTP-порты	80,81,8000:8900 ✓

Рисунок 76. Уровень эвристического анализа

На вкладке *Эвристика* (см. Рисунок 77) 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*.

Опции	Несигнатурные угрозы	COB	МЭ	Пресеты	Обновить	Настройка config файла
Фрагментация	Сканирование портов	Эвристика				
Включить эвристику DNS-тоннелей ☒						
Уровень чувствительности Низкий Низкий Средний Высокий						
Сохранить		Применить		Сбросить		

Рисунок 77. Несигнатурные угрозы. Эвристика

На вкладке *COB* (см. Рисунок 78) приведена информация о состоянии *Средства обнаружения вторжений*, о количестве активных правил, общем количестве настроенных правил, количестве правил из *Базы решающих правил*. Ниже представлены правила (База решающих правил), которые можно отдельно настраивать. Существует возможность изменить правила под свою инфраструктуру, задав уточняющие данные, либо включить/отключить составляющие политики для правил.

Для включения или отключения нескольких правил одновременно следует нажать кнопку **Выбрать правила**, выбрать нужные правила и нажать соответствующую кнопку.

Фильтр содержимого ⓘ

Опции Несигнатурные угрозы **COB** МЭ Пресеты Обновить Настройка config файла

☐ Включить COB 0 / 14992 / 14992 активно / настроено / БРП

Пресет ^ IP ^ Фильтр правил... Фильтр Выводить по: 10 ☐ Только включенные Сбросить фильтры 0 / 10 / 10

Отменить Включить Отключить Добавить в пресет... Отметить как просмотренные

Включено	Название правила	Действие
☒	test ddos [0301]	DoS/DDoS
☐	MySQL Попытка внедрить произвольную библиотеку [0902]	Инъекция
☐	FTP INTO OUTFILE SQL инъекция [0926]	Инъекция
☐	Аномальная фрагментация ICMP [1003]	
☐	Установлен незначимый флаг фрагментации [1005]	
☐	Фрагментация IGMP [1006]	
☐	Фрагментация с наложением (Teardrop) [1007]	
☐	Несовместимые параметры фрагментации [1008]	
☐	Разбиение на крошечные фрагменты [1009]	
☐	SERVER-APACHE Apache Struts remote code execution attempt - POST parameter [1229]	

Сохранить Применить Сбросить

Рисунок 78. Фильтр содержимого — COB

COB управляет сетевым трафиком к устройствам в LAN и DMZ зонах, основываясь на наборах правил, которые определяют, как обрабатывать входящие и исходящие пакеты данных. В зависимости от параметров правила COB, возможны следующие действия с трафиком:

- Отвергнуть (reject). Трафик блокируется, но отправителю сообщается, что его пакет не был доставлен.
- Заблокировать (block). Трафик блокируется без уведомления отправителя.
- Пропустить (pass). Трафик разрешается и проходит через межсетевой экран.
- Тревога (alert). Трафик разрешается, но при этом фиксируется в журнале для последующего анализа.

Для удобства администрирования UTM правила объединены в отдельные категории (пресеты). Пресеты содержат в себе правила обработки сетевого трафика. Для изменения правила под свою инфраструктуру необходимо выбрать правило и нажать кнопку **Изменить** (см. Рисунок 79), в списке настроить параметры для сети. Для сохранения параметров нажать кнопку **Сохранить**.

Для добавления дополнительной настройки правила нажать кнопку **Добавить**, внести соответствующие изменения в параметры и нажать кнопку **Сохранить** (см. Рисунок 79). Для удаления настройки правила, нажать на кнопку **Удалить**.

☒ test ddos [0301] DoS/DDoS

Включено	Действие	Источник	Направление	Действия
☒	Отвергнуть	IP-адрес: EXTERNAL_NET Порт: любой	IP-адрес: любой Порт: любой	Изменить Удалить

Добавить +

Рисунок 79. Параметры правила COB

Страница изменения и просмотра правила COB содержит поля аналогичные странице изменения и просмотра правила WAF (см. 5.1.4 Фильтр содержимого).

Предустановленные пресеты COB нацелены на предотвращение распространенных атак (см. Таблица 6).

Таблица 6. Пресеты COB

Наименование пресета	Назначение
! DoS/DDoS	защита DoS/DDoS атак
! Инъекции	защита от SQL-инъекций
APP-DETECT	обнаружение трафика, генерируемого определенными приложениями, работающими в сети
BROWSER-CHROME	обнаружение трафика, содержащего попытки использования уязвимостей или особенностей работы браузера Chrome
BROWSER-FIREFOX	обнаружение трафика, содержащего попытки использования уязвимостей или особенностей работы браузера Mozilla Firefox
BROWSER-IE	обнаружение трафика, содержащего попытки использования уязвимостей или особенностей работы браузера Internet Explorer
BROWSER-OTHER	обнаружение трафика, содержащего попытки использования уязвимостей или особенностей работы браузеров (в основном Opera)
BROWSER-PLUGINS	обнаружение трафика, содержащего попытки использования уязвимостей или особенностей работы плагинов веб-браузеров
BROWSER-WEBKIT	обнаружение трафика, содержащего попытки использования уязвимостей или особенностей работы браузеров построенных на основе Webkit
EXPLOIT-KIT	обнаружение трафика, с использованием сигнатур известных эксплоитов
FILE-EXECUTABLE	обнаружение трафика, содержащего уязвимости в исполняемых файлах
FILE-FLASH	обнаружение подозрительного трафика к Adobe Flash Player
FILE-IDENTIFY	обнаружение файлов с определенным идентификатором в трафике
FILE-IMAGE	обнаружение трафика, нацеленного на эксплуатацию уязвимостей в файлах изображений
FILE-JAVA	обнаружение трафика, нацеленного на эксплуатацию уязвимостей в Java-файлах
FILE-MULTIMEDIA	обнаружение трафика, нацеленного на эксплуатацию уязвимостей в мультимедийных файлах
FILE-OFFICE	обнаружение трафика, нацеленного на эксплуатацию уязвимостей в файлах офисных программ
FILE-OTHER	обнаружение трафика, нацеленного на эксплуатацию уязвимостей в различных файлах
FILE-PDF	обнаружение трафика, нацеленного на эксплуатацию уязвимостей в PDF-файлах
INDICATOR-COMPROMISE	обнаружение трафика, содержащего опасные запросы к удаленным ресурсам
INDICATOR-OBFUSCATION	обнаружение обфусцированного JS кода в трафике
INDICATOR-SCAN	обнаружение трафика, содержащего попытки сканирования сети
INDICATOR-SHELLCODE	обнаружение трафика, содержащего в пакетах фрагмент машинного кода
MALWARE-BACKDOOR	обнаружение трафика, содержащего запрос соединения с удаленным компьютером, инициализированный вредоносным ПО
MALWARE-CNC	обнаружение трафика от центра управления множеством компьютеров
MALWARE-CNC User-Agent	
MALWARE-CNC Win	
MALWARE-OTHER	обнаружение трафика, связанного с работой вредоносного ПО, не подпадающего под описание предыдущих четырех пунктов
MALWARE-TOOLS	обнаружение трафика, связанного с работой хакерского инструментария
OS-LINUX	обнаружение трафика, эксплуатирующего уязвимости операционных систем семейства Linux
OS-MOBILE	обнаружение трафика, эксплуатирующего уязвимости мобильных операционных систем

Наименование пресета	Назначение
OS-OTHER	обнаружение трафика, эксплуатирующего уязвимости операционных систем
OS-SOLARIS	обнаружение трафика, эксплуатирующего уязвимости операционной системы Solaris
OS-WINDOWS	обнаружение трафика, эксплуатирующего уязвимости операционных систем семейства Windows и их компонентов
POLICY-MULTIMEDIA	обнаружение трафика к мультимедийным ресурсам
POLICY-OTHER	обнаружение трафика к определенным ресурсам
POLICY-SOCIAL	обнаружение трафика к социальным сетям
POLICY-SPAM	обнаружение трафика, содержащего спам сообщения
PROTOCOL-SCADA	обнаружение ошибок и потенциальных атак на SCADA-системы
PUA-ADWARE	идентификация потенциально нежелательных приложений, связанных с размещением рекламы
PUA-OTHER	идентификация потенциально нежелательных приложений
PUA-P2P	идентификация потенциально нежелательных приложений, которые используют пиринговые сети (P2P) для обмена файлами (например, торрент-трекеров)
PUA-TOOLBARS	идентификация потенциально нежелательных приложений, таких как нежелательные панели инструментов в веб-браузерах
SERVER-APACHE	обнаружение трафика, эксплуатирующего уязвимости веб-серверов Apache
SERVER-IIS	обнаружение трафика, эксплуатирующего уязвимости веб-серверов IIS
SERVER-MAIL	обнаружение трафика, эксплуатирующего уязвимости почтовых серверов организации
SERVER-MSSQL	обнаружение трафика, эксплуатирующего уязвимости сервера баз данных под управлением MSSQL
SERVER-ORACLE	обнаружение трафика, эксплуатирующего уязвимости сервера баз данных под управлением Oracle
SERVER-OTHER	обнаружение трафика, эксплуатирующего уязвимости веб-приложений
SERVER-WEBAPP	защита популярных веб-приложений от атак, связанных с эксплуатацией уязвимостей
SERVER-WEBAPP WECON	защита контроллеров Wecon от атак, связанных с эксплуатацией уязвимостей
SERVER-WEBAPP WordPress	защита системы управления содержимым WordPress от атак, связанных с эксплуатацией уязвимостей
SQL	защита веб-серверов от SQL-инъекций

На вкладке МЭ (см. Рисунок 80) 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.

Для включения или отключения нескольких правил одновременно следует нажать кнопку **Выбрать правила**, выбрать нужные правила и нажать соответствующую кнопку.

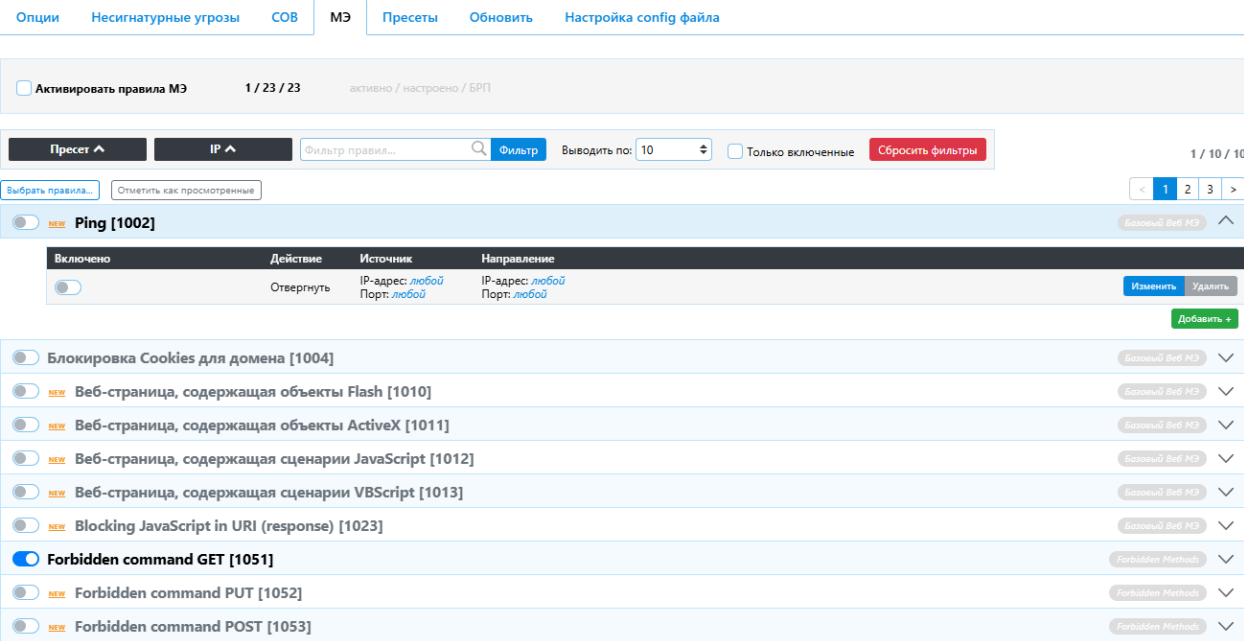


Рисунок 80. Межсетевой экран

Для изменения правила под свою инфраструктуру необходимо выбрать правило и нажать кнопку **Изменить** (см. Рисунок 81), в списке настроить параметры для сети. Для сохранения параметров нажать кнопку **Сохранить**.
 Для добавления дополнительной настройки правила нажать кнопку **Добавить**, внести соответствующие изменения в параметры и нажать кнопку **Сохранить** (см. Рисунок 79). Для удаления настройки правила нажать на кнопку **Удалить**.
 Страница изменения и просмотра правила МЭ содержит поля аналогичные странице изменения и просмотра правила WAF (см. 5.1.4 Филтър содержимого).

Forbidden command GET [базовое правило]

Включено

ID / Ревизия

1051 / 1

Пресет (приложение)

http

Тип события безопасности

—

Уровень атаки

Средний [2]

Тип трафика

HTTP

Протокол нижнего уровня

TCP

Действие

Отвергнуть [reject]

Источник

Любой

Порт источника

Любой

Направление

Любой

Порт назначения

Любой

Правила контекстного филтра

```
[
  {
    "content": {
      "options": {
        "http_method": "y"
      },
      "string": "GET"
    }
  },
  {
    "": "y"
  }
]
```

Назад

Применить

Сбросить

Рисунок 81. Параметры правила МЭ

Предустановленные пресеты МЭ предназначены для защиты сети от различных угроз (см. Таблица 7).

Таблица 7. Пресеты МЭ

Наименование пресета	Назначение
Базовый Веб МЭ	защита от трафика, содержащего ICMP-запросы и интерактивный контент
Forbidden Data	обнаружение трафика, содержащего текстовый контент определенных кодировок и нетекстовый контент
Forbidden Methods	обнаружение трафика, содержащего методы HTTP

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 82).



Правила пресета Forbidden Data и Forbidden Methods являются сервисными пресетами. Их включение приводит к коду ответа 403 при обращении к любым HTTP/HTTPS серверам со стороны зон LAN и WAN, в том числе при обращении к защищаемому ресурсу.

Опции
Несигнатурные угрозы
COB
МЭ
Пресеты
Обновить
Настройка config файла

Пользовательские пресеты

Название пресета	Custom	Удалить секцию
Включить базовые правила для всех	☒	0 правил(0,0)

Добавить +

Пресеты

Название пресета	Dos/DDos	Удалить секцию
Включить базовые правила для всех	☒	7 правил(0,0)

APP-DETECT [47] Добавить +

Сохранить
Применить
Сбросить

Рисунок 82. Пресеты



Включение большого количества пресетов может существенно увеличить нагрузку на межсетевой экран, что может привести к замедлению обработки трафика веб-сервера. Это связано с тем, что каждый пресет добавляет дополнительную логику и проверки, которые необходимо выполнить. Поэтому важно активировать только те пресеты, которые действительно необходимы для данной инфраструктуры и используемых технологий.

Кроме предустановленных пресетов можно создавать и собственные. Для этого доступны следующие способы создания пресетов:

- Создать пресет на вкладке *Пресеты*:
 - Нажать кнопку **Добавить** в блоке *Пользовательские пресеты*.
 - Ввести имя пресета и установить чекбокс *Включить базовые правила для всех*.
 - Перейти на вкладку *МЭ* или *COB* и нажать кнопку **Выбрать правила**.
 - Выбрать нужные правила.

- Нажать кнопку **Добавить в пресет**.
 - Выбрать ранее созданный пресет.
 - Нажать кнопку **Добавить**, чтобы добавить правила в пресет.
2. Создать пресет на вкладке *МЭ* или *СОВ*:
- Нажать кнопку **Выбрать правила**.
 - Выбрать нужные правила.
 - Нажать кнопку **Добавить в пресет**.
 - Для создания нового пресета в поле *Пресеты* выбрать *Новый пресет* и ввести его имя (см. Рисунок 83).
 - Нажать кнопку **Добавить**, чтобы правила были добавлены в новый пресет, который отобразится на вкладке *Пресеты*.

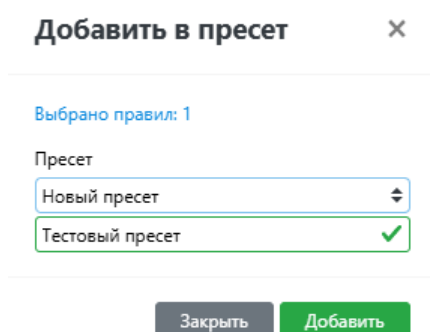


Рисунок 83. Добавление пресета

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 84).



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 правил и их применения к защищаемым ресурсам и отдельным узлам сети.

Фильтр содержимого i

Опции
Несигнатурные угрозы
СОВ
МЭ
Пресеты
Обновить
Настройка config файла

По сети Интернет

URL	https://updates.dallaslock.ru/WafUpdate/utm-brp-current.tar.gz
Обновить данные	Обновить
Регулярно по расписанию	☐

Из файла

Загрузить

Рисунок 84. Обновить

Вкладка *Настройка config-файла* будет полезна в случае ручного описания файла конфигурации правил для UTM (см. Рисунок 85).

Фильтр содержимого



Опции
Несигнатурные угрозы
СОВ
МЭ
Пресеты
Обновить
Настройка config файла

```

#
# Custom rule for UTM
#

# pattern
#alert tcp any any -> any $HTTP_PORTS (msg:"[:IDS:100:2:] Cookie block by domain";content:"google.com";pcr:"/\;\/s*domain=google.com/i";sid:1000002)

#reject tcp any $HTTP_PORTS <> any any (msg:"[:FW:201:3:] Cookie block by domain";content:"cookie:";nocase;pcr:"/\;\/s*domain=.google.com/i";sid:11004090;rev:3;)
#reject tcp any any <> any $HTTP_PORTS (msg:"[:FW:202:3:] Host block by domain";content:"host:";nocase;pcr:"/youtube.com/i";sid:11004091;rev:3;)

#####
# Step #8: Customize your preprocessor and decoder alerts
#####

# decoder and preprocessor event rules
# include $UTM_RULE_PATH/http_inspect.conf
# include $PREPROC_RULE_PATH/preprocessor.rules
# include $PREPROC_RULE_PATH/decoder.rules
# include $PREPROC_RULE_PATH/sensitive-data.rules

```

Применить
Сбросить

Рисунок 85. Настройка config файла

5.3 Настройки модуля ЕЦУ

5.3.1 Единый центр управления Dallas Lock

Для реализации централизованного управления **WAF Dallas Lock** необходимо использовать **Единый центр управления Dallas Lock (ЕЦУ Dallas Lock)**, управление которым осуществляется отдельным приложением **Консоль ЕЦУ**.

ЕЦУ Dallas Lock позволяет осуществлять централизованное управление такими модулями клиентов, как шлюз безопасности **WAF Dallas Lock**, **СЗИ Dallas Lock 8.0** редакций «К» и «С», **СЗИ Dallas Lock Linux**, **СЗИ ВИ Dallas Lock**, **СДЗ Dallas Lock** и **СДЗ УБ Dallas Lock**.

При работе со шлюзом безопасности **WAF Dallas Lock** доступны следующие возможности:

- завершение работы и перезагрузка модуля;
- отображение информации о состоянии модуля (состояние подключения, режим работы, имя шлюза безопасности, IP-адрес шлюза безопасности, анализ журналов событий шлюза безопасности, MAC-адрес подключения шлюза безопасности, данные об аппаратном обеспечении, версия ПО, версия базы решающих правил, объем свободного места на диске, номер лицензии, код технической поддержки);
- перевод шлюза безопасности в режиме кластера в состояние Master;
- сброс временных блокировок;
- однокомандное управление активацией и деактивацией аварийного режима;
- открытие веб-интерфейса администрирования;
- управление заданиями на:
 - обновление базы решающих правил;
 - создание и восстановление резервной копии;
 - сброс к заводским настройкам;
 - применение файла лицензии;
- сбор журналов модуля;
- сигнализация и мониторинг инцидентов безопасности с графическим отображением.

Некоторые параметры безопасности могут быть настроены сразу для всего **ДБ**, некоторые — для

отдельных клиентов.

С подробным описанием **ЕЦУ Dallas Lock** можно ознакомиться в Инструкции по использованию ЕЦУ Dallas Lock (ПФНА.26.20.40.143.001 ИЗ).

5.3.2 Регистрация WAF Dallas Lock в домене безопасности ЕЦУ

Для регистрации в домене безопасности **ЕЦУ** в основном меню в разделе **Настройки** следует выбрать пункт **Настройки модуля ЕЦУ** (см. Рисунок 86).

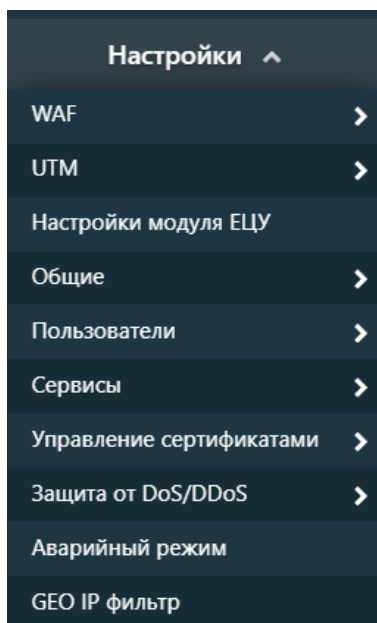


Рисунок 86. Раздел настроек, пункт Настройки модуля ЕЦУ

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 87). Для сохранения введенных настроек в форме веб-интерфейса необходимо нажать кнопку **Сохранить**.



Статус

НЕ ЗАРЕГИСТРИРОВАН

Обновить данные
Обновить

Настройки

Имя модуля	WAF21014	✓	
Сервер ЕЦУ	192.168.157.3	✓	
Ключ доступа к ДБ		👁	
Зарегистрировать в ДБ	Зарегистрироваться		

Сохранить

Рисунок 87. 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 88), а в блоке **Статус** появится информация о сервере **ЕЦУ Dallas Lock** (см. Рисунок 89).

Настройки

Имя модуля	WAF21014	✓
Сервер ЕЦУ	192.168.157.3	✓
Ключ доступа к ДБ	*****	👁
Вывести из ДБ	Вывести из ДБ	

Рисунок 88. Регистрация шлюза безопасности в ДБ прошла успешно

Статус

Имя домена безопасности	Домен безопасности
Имя сервера безопасности	UCCARM1:17900
Введен в ДБ как	WAF Dallas Lock ИК2
Обновить данные	Обновить

Рисунок 89. Блок Статус 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** в блоке настроек *Состояние* будет не активна.

Чтобы вывести устройство из ДБ, необходимо нажать кнопку **Вывести из ДБ** (см. Рисунок 88) и подтвердить действие во всплывающем окне, нажав кнопку **ОК**. После этого 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.

5.4 Общие настройки

5.4.1 Система

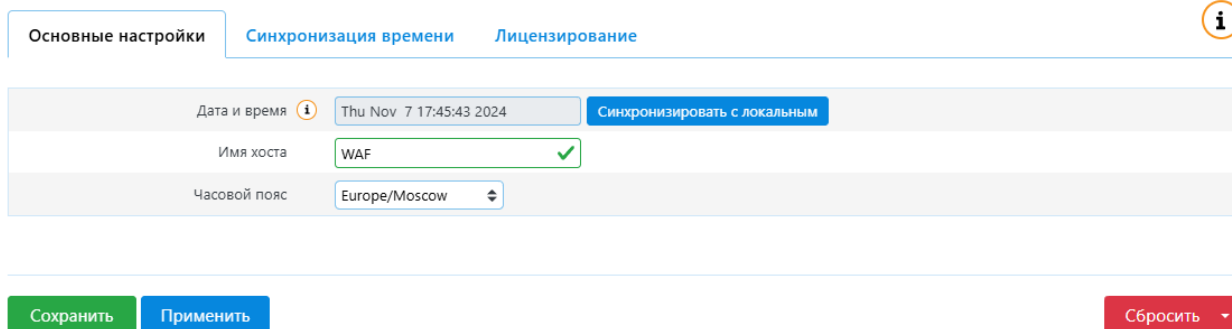
На данной странице можно задать параметры устройства, такие как дата и время, имя хоста, часовой пояс, код лицензии и технической поддержки. (см. Рисунок 90)

Вкладка *Основные настройки*:

Дата и время. Текущая дата и время.

Имя Хоста. Позволяет задать имя хоста.

Часовой пояс. Позволяет выбрать часовой пояс.



Основные настройки Синхронизация времени Лицензирование

Дата и время Thu Nov 7 17:45:43 2024 Синхронизировать с локальным

Имя хоста WAF ✓

Часовой пояс Europe/Moscow

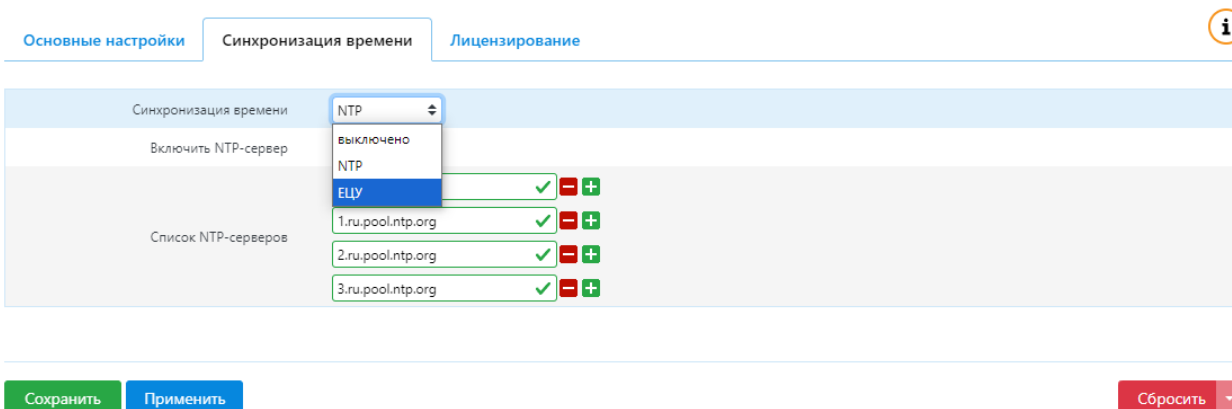
Сохранить Применить Сбросить

Рисунок 90. Основные настройки

Синхронизация времени.

На данной вкладке (см. Рисунок 91) можно указать адрес NTP-сервера, который будет передавать временные метки для журналирования. Для этого необходимо выполнить следующие действия:

1. В строке *Синхронизация времени* выбрать *NTP*.
2. Поставить чекбокс напротив *Включить NTP-сервер*.
3. В строке *Список NTP-серверов* задать IP-адрес или имя сервера времени.



Основные настройки Синхронизация времени Лицензирование

Синхронизация времени NTP

Включить NTP-сервер ☒

Список NTP-серверов

ЕЦУ	✓	-	+
1.ru.pool.ntp.org	✓	-	+
2.ru.pool.ntp.org	✓	-	+
3.ru.pool.ntp.org	✓	-	+

Сохранить Применить Сбросить

Рисунок 91. Синхронизация времени



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

Вкладка *Лицензирование* (см. Рисунок 92) позволяет пользователю получить информацию о примененной лицензии продукта, подключенных модулях защиты, дате окончания срока лицензии. В строке *Загрузка файла лицензии* можно загрузить файл лицензии, нажав кнопку «...», и удалить, нажав кнопку **Удалить лицензию**.

Основные настройки

Синхронизация времени

Лицензирование

Загрузка файла лицензии

...

Макс. размер: 10.00 КВ

Удалить лицензию

Информация о лицензии

Номер лицензии / Код поддержки	000000000-0000-00000 / 000000000-000
Истекает	23.08.2027
Модули	COB WAF Кластер 3000RPS

Сохранить

Применить

Сбросить

Рисунок 92. 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 93);
- загрузить файл лицензии, выполнив переход на вкладку *Лицензирование* раздела меню **Основные**, подробнее в разделе [5.4.1 Система](#) (см. Рисунок 93);
- включить/выключить доступ по протоколу SSH (см. Рисунок 94). По умолчанию доступ по протоколу SSH выключен;
- сконфигурировать доступ к сервису SSH (см. Рисунок 94), указав в настройках:
 - *Интерфейс*. Можно указать, через какой сетевой интерфейс будет возможно подключение к **WAF Dallas Lock** по протоколу 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 администратора (root) и внутреннего пользователя (subadmin) **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.



Если функция аутентификации по паролю отключена, доступ по протоколу SSH возможен только с использованием заранее сгенерированных публичных SSH-ключей, добавленных в поле *SSH-ключи*.

Для каждого интерфейса задаются отдельные настройки. Для того чтобы добавить интерфейс необходимо нажать кнопку **Добавить секцию**, выбрать интерфейс и указать настройки.

Настройки интерфейса управления WAF DL



Базовые Web-интерфейс Управл. доступом к МЭ

Пароль администратора

Пароль		
Подтверждение		

Загрузка файла лицензии

Рисунок 93. Пароль администратора. Загрузка файла лицензии.

Конфигурация сервиса SSH

Доступ по SSH ☐

Интерфейс

- ☐ dmz:
- ☐ lan:
- ☐ wan:
- ☐ wan6:
- ☒ включить доступ по всем интерфейсам

Порт 22

С помощью пароля ☒

Таймаут неактивной сессии 15 мин.

Добавить секцию

SSH-ключи

Сохранить Применить Сбросить

Рисунок 94. Конфигурация сервиса SSH



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

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. Доступ по протоколу SSH предоставляется только администратору (root) и внутреннему пользователю (subadmin).

Доступна одновременная авторизация через консоль управления по протоколу SSH и через веб-интерфейс. Так же есть возможность использовать эмулятор терминала Linux ISH Shell (консольная оболочка администрирования) на самом сервере **WAF Dallas Lock**.

Сценарии:

- Администратор производит авторизацию с клиентского ПК на **WAF Dallas Lock** через веб-интерфейс или через SSH (подключение через SSH должно быть разрешено);
- Также администратор может одновременно открыть сессию на самом сервере **WAF Dallas Lock** и производить настройки в консольной оболочке.



Для обеспечения безопасности доступ к конфигурированию через консольную оболочку по протоколу SSH, а также напрямую на сервере ограничен командами ISH Shell (консольной оболочки администрирования **WAF Dallas Lock**). Команды конфигурирования доступны исключительно администратору (root), в то время как внутренний пользователь (subadmin) может выполнять только команды для просмотра информации о системе.



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 (см. Таблица 8). Список служб и их описание представлены в разделе [5.4.6 Управление службами](#) (см. Таблица 9).

Таблица 8. Список команд

Команда	Описание	Параметры/команды
<i>help</i>	Выводит полный список команд, доступных на текущем уровне (напротив каждой команды следует пояснение)	отсутствуют
<i>exit</i>	Выход с любого уровня оболочки с необходимостью авторизации после выхода	отсутствуют
<i>list</i>	Список команд доступных на текущем уровне	отсутствуют
<i>return</i>	Переход на верхний уровень в иерархии оболочки (на самом верхнем уровне не происходит никакого действия)	отсутствуют
<i>waf-settings</i>	Переход на уровень конфигурирования WAF Dallas Lock	отсутствуют
Команды уровня waf-settings (выполнение разрешено только администратору)		
<i>backup-config</i>	Команда сохранения резервного архива текущей конфигурации	<i>path</i> — строковая величина: указывается путь и имя файла для сохранения в него архива конфигурации <i>Пример:</i> <i>backup-config <enter></i> <i>path "/путь/имя файла" <enter></i>
<i>backup-logs</i>	Команда сохранения резервного архива журналов на локальном жестком диске	отсутствуют
<i>emerge-off</i>	Команда выключения аварийного режима	отсутствуют
<i>emerge-on</i>	Команда включения аварийного режима	отсутствуют
<i>factory-reset</i>	Команда сброса системы к заводским установкам	отсутствуют
<i>load-rj</i>	Загрузка правил	<i>all</i> — булева величина в формате yes/no: загрузка всех правил;

Команда	Описание	Параметры/команды
		<i>force</i> — булева величина в формате yes/no: обязательность загрузки правил; <i>utm</i> — булева величина в формате yes/no: правила UTM; <i>utm_rev2</i> — булева величина в формате yes/no: правила UTM rev.2 (при сбросе на заводские настройки); <i>waf</i> — булева величина в формате yes/no: правила WAF; <i>waf_rev2</i> — булева величина в формате yes/no: правила WAF rev.22 (при сбросе на заводские настройки). <i>Пример:</i> <i>load-rj <enter></i> <i>all yes <enter></i>
<i>maintenance</i>	Зарезервированная команда	отсутствуют
<i>mgmt-ip</i>	Добавление IP-адреса в список адресов, с которых возможно администрирование системы	<i>ip</i> — строковая величина: указывает IP-адрес <i>Пример:</i> <i>mgmt-ip <enter></i> <i>ip "IP-адрес" <enter></i>
<i>reboot</i>	Перезагрузка системы	отсутствуют
<i>reset-logs</i>	Удаление журналов	отсутствуют
<i>resize-var</i>	Оптимизация размера /var (расширение раздела для хранения журналов на весь жесткий диск)	отсутствуют
<i>restart-service</i>	Перезапуск сервиса	<i>service</i> — строковая величина: указывает наименование сервиса для перезагрузки <i>Пример:</i> <i>restart-service <enter></i> <i>service "название_сервиса" <enter></i>
<i>shutdown</i>	Выключение системы	отсутствуют
<i>syslog-archive</i>	Архивирование системных журналов в файл с датой в имени в директорию /var/archive/syslog	отсутствуют
<i>create-subadmin</i>	Создание учетной записи пользователя subadmin и группы subadmin для администрирования сервера	отсутствуют
<i>remove-subadmin</i>	Удаление учетной записи пользователя subadmin и группы subadmin для администрирования сервера	отсутствуют
<i>web-ui</i>	Команда перехода на уровень управления веб-интерфейсом	<i>client-auth-disable</i> — команда отключения режима авторизации администратора с

Команда	Описание	Параметры/команды
		использованием SSL-сертификата; <i>cert-reset</i> — команда перезагрузки службы веб-интерфейса в безопасном режиме
Команды уровня waf-settings (выполнение разрешено администратору (root) и внутреннему пользователю (subadmin))		
<i>get-cpuload</i>	Вывод на экран суммарной загрузки процессора на момент вызова команды	отсутствуют
<i>get-freediskspace</i>	Вывод на экран количества байт свободного места на диске	отсутствуют
<i>get-freemem</i>	Вывод на экран количества байт свободной оперативной памяти на момент вызова команды	отсутствуют
Команды конфигурирования		
<i>execute</i>	Вызов команды	
<i>preview</i>	Просмотр параметров конфигурируемой команды	
Команды синонимы (alias)		
<i>r — return</i>	Переход на верхний уровень в иерархии оболочки	отсутствуют
<i>x — exit</i>	Команда выполняет выход с любого уровня оболочки, с необходимостью авторизации после выхода	отсутствуют

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 95):

- *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 на публичном интерфейсе.* Эта функция не позволяет подделывать 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).

Базовые
Web-интерфейс
Управл. доступом к МЭ

Основные настройки
Дополнительные настройки ⓘ
Сертификат HTTPS
Аутентификация по сертификату

Входящие HTTP (адрес:порт) ⓘ - +

Входящие HTTPS (адрес:порт) ⓘ ✓ - +

✓ - +

Игнорировать приватные IP-адреса на публичном интерфейсе ⓘ ☒

Сохранить
Применить
Сбросить

Рисунок 95. Основные настройки

Дополнительные настройки. Задаются дополнительные настройки сессии администратора при авторизации к интерфейсу **WAF Dallas Lock** по протоколу HTTPS (см. Рисунок 96).

Базовые
Web-интерфейс
Управл. доступом к МЭ

Основные настройки
Дополнительные настройки ⓘ
Сертификат HTTPS
Аутентификация по сертификату

Страница содержит параметры, которые редко используются или влияют на обслуживание веб-интерфейса.

Время действия авторизации ⓘ	15	✓	мин
Максимальное время ожидания загрузки ⓘ	60	✓	сек
Максимальное время ожидания сетевой активности ⓘ	30	✓	сек
Открыть доступ к UI на ⓘ	12	✓	ч
Повторное использование соединения ⓘ	0	✓	сек
TCP Keepalive ⓘ	100	✓	сек
Максимальное количество соединений ⓘ	500	✓	
Максимальное количество запросов скрипта ⓘ	100	✓	

Сохранить
Применить
Сбросить

Рисунок 96. Дополнительные настройки

- **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.

Сертификат HTTPS. На данной вкладке (см. Рисунок 97) 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.



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

Базовые
Web-интерфейс
Управл. доступом к МЭ

Основные настройки
Дополнительные настройки
Сертификат HTTPS
Аутентификация по сертификату

Сертификат HTTPS [utm]	Загруженный файл (4.19 KB) Макс. размер: 142.33 MB	uhttpd.crt (15.10.2024, 17:54) Отпечаток: e13f451e
	Посмотреть	Обновить локально
Приватный ключ HTTPS	Загруженный файл (1.64 KB) Макс. размер: 142.33 MB	uhttpd.key (15.10.2024, 17:54)
Имя хоста	WAFIK2.dl.local	
Запрос подписания сертификата	Скачать	

Сохранить
Применить
Сбросить

Рисунок 97. Сертификат HTTPS



В строке *имя хоста* использование «.» в имени сервера при аутентификации по сертификату *CA Root* приводит к предупреждению, что сертификат недействителен (см. Рисунок 98). При этом полное имя сервера *host.local*, где *local* имя домена, не приводит к подобной ошибке.

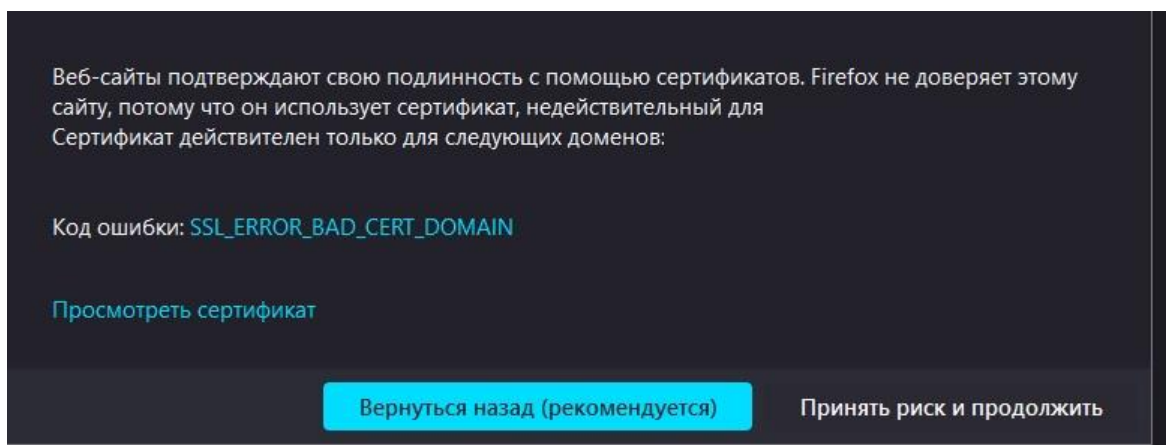


Рисунок 98. Ошибка SSL сертификата

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 99).

Базовые
Web-интерфейс
Управл. доступом к МЭ

Основные настройки
Дополнительные настройки
Сертификат HTTPS
Аутентификация по сертификату

Включить аутентификацию по сертификату	☒
Сертификат	Макс. размер: 142.32 MB

Сохранить
Применить
Сбросить

Рисунок 99. 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 ключ 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 99) 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 автоматизированном рабочем месте установлена **СЗИ НСД Dallas Lock 8.0**. В противном случае могут возникнуть проблемы в процессе аутентификации **WAF Dallas Lock**, и потребуются вносить дополнительные настройки в реестр операционной системы.

5.4.2.3 Управление доступом к межсетевому экрану

На вкладке **Управление доступом к МЭ** (см. Рисунок 100) 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 Dallas Lock**.
- *Новое правило доступа*. Данная функция позволяет добавить IP-адрес клиента для доступа к веб-интерфейсу из внешней сети. Для этого нужно ввести внешний IP-адрес/Сеть и нажать кнопку **Добавить** (см. Рисунок 100).

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



При необходимости конфигурирования **WAF Dallas Lock** из зон WAN и DMZ рекомендуется добавлять зарезервированные IP-адреса компьютеров в список *Дополнительный доступ* при значении параметра *Ограничить доступ только с интерфейса* «LAN».

Базовые
Web-интерфейс
Управл. доступом к МЭ

Ограничить доступ только с интерфейса ⓘ LAN

Дополнительный доступ ⓘ

Имя	Разрешить доступ	Включить	
access001	с IP 192.168.131.81	☒	Изменить Удалить

Новое правило доступа

Внешний IP-адрес / Сеть	
Внешний IP-адрес / Сеть	Добавить

Сохранить Применить Сбросить

Рисунок 100. Управление доступом

После того как внешний IP-адрес добавлен, откроется страница настройки созданного правила доступа (см. Рисунок 101), где можно задать производное имя сети, а также включить/отключить правило.

Базовые
Web-интерфейс
Управл. доступом к МЭ

Предупреждение: при сохранении настроек вы можете потерять доступ к управлению.

Межсетевой экран - Параметры управления доступом - access001 ⓘ

Правило включено	Отключить
Имя	access001
Внешний IP-адрес / Сеть ⓘ	192.168.131.81 ✓

Назад Сохранить Применить Сбросить

Рисунок 101. Параметры управления доступом


При сохранении настроек доступ к управлению может быть утерян.

5.4.3 Параметры аудитора

Страница *Параметры аудитора* доступна из основного меню (см. Рисунок 102). Содержит настройки аудита и обработки инцидентов безопасности. На странице доступны следующие вкладки:

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

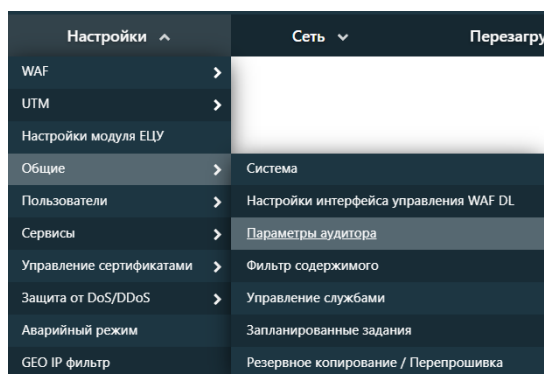


Рисунок 102. Параметры аудитора

Вкладка *Настройка журнала* (см. Рисунок 103) позволяет выбрать какие типы событий безопасности будут записываться в журналы, а также параметры для журналирования на удаленный сервер:

Записывать в журнал. 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 «error (Ошибка)» в журналы будут записываться типы событий: error (Ошибка), crit (Критическая ситуация), alert (Тревога), emerg (Чрезвычайная ситуация).

- *Протокол внешнего лог-сервера.* Выпадающий список для выбора протокола транспортного уровня (UDP/TCP/UDP (IEFT-syslog)/TCP (IEFT-syslog)) 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**.

Настройка журнала
Архивирование журналов
Обработка инцидентов

Уровень логирования	debug (Отладка)
Протокол внешнего лог-сервера	UDP
Адрес внешнего лог-сервера	loghost.local
Порт внешнего лог-сервера	514
Уровень логирования на внешний сервер	debug (Отладка)
Включить внешний LEEF-сервер	☒
Адрес внешнего LEEF-сервера	leef.local
Порт внешнего LEEF-сервера	514
Непрерывная отправка журналов в ЕЦУ	☒
Уровень логирования ЕЦУ	notice (Заметка)

Сохранить
Применить
Сбросить

Рисунок 103. Настройка журнала

Вкладка *Архивирование журналов* (см. Рисунок 104) позволяет создать, скачать, загрузить и удалить архивированные журналы.

Настройка журнала
Архивирование журналов
Обработка инцидентов

Размер журналов аудита	100 MB
------------------------	--------

Архивирование журналов
Создать архив

Архивирование текущих журналов
☐

2024-10-18 15:12:19	6.927 kB	Скачать	Удалить
---------------------	----------	---------	---------

Загрузить архив журналов
Загрузка

Очистить загруженные журналы
Удалить

Перейти к просмотру журналов

Рисунок 104. Архивирование журналов



На данной странице кнопки **Создать архив**, **Скачать**, **Удалить** (см. Рисунок 105) 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 105):

- **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 атрибуты (см. Рисунок 105):

- **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.

2024-10-18 15:12:19	6.927 kB	Скачать	Удалить
2024-10-18 15:13:24	1.688 kB	Скачать	Удалить

Рисунок 105. Архивированные журналы

Для загрузки архива журналов необходимо (см. Рисунок 106):

1. Нажать кнопку **Загрузка**;
2. Выбрать архивированный журнал из архивов журналов на ПК;
3. Повторно нажать кнопку **Загрузка**;
4. В таблице **Список журналов в архиве для загрузки** появятся следующие поля:
 - *Чекбокс.* Для выбора журнала и выполнения 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*.

Загрузить архив журналов		...	Загрузка
Макс. размер: 142.37 MB			
Очистить загруженные журналы	Удалить		
Перейти к просмотру журналов			

Список журналов в архиве для загрузки

	Журнал: Все	Дата архивации	Размер
☐	Политики	2024-10-18 15:12:19	4.0K
☐	Системный	2024-10-18 15:12:19	4.0K
☐	Системный	2024-10-18 15:10:00	4.0K
☐	Политики	2024-10-18 15:10:00	4.0K
☐	Сетевые пакеты	2024-10-18 15:10:00	4.0K
☐	СОВ	2024-10-18 15:10:00	4.0K
☐	WAF	2024-10-18 15:10:00	4.0K
☐	МЭ	2024-10-18 15:10:00	4.0K

Рисунок 106. 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**.

Вкладка *Обработка инцидентов* (см. Рисунок 107) 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, происходит 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 достижении которого **WAF Dallas Lock** блокирует IP-адрес источника событий.
- **Время ожидания повторов.** Период времени в минутах, в течение которого отслеживаются события одного типа.

Настройка журнала
Архивирование журналов
Обработка инцидентов

Ограничение для пользователя на попытки входа ⓘ

Превышение попыток входа	5	✓
Таймаут	15	✓ мин

Ограничение доступа по IP для пользователя при подозрении на DOS-атаку ⓘ

Превышение попыток входа	10	✓
Таймаут	60	✓ мин

Ограничения по видам угроз в трафике

Высокий уровень ⓘ	22	✓
Средний уровень ⓘ	30	✓
Низкий уровень ⓘ	100	✓

Ограничения по ошибкам на защищаемом ресурсе ⓘ

Превышение событий	300	✓
--------------------	-----	---

Другие виды событий ⓘ

Число событий	10	✓
Время ожидания повторов ⓘ	25	✓ мин

Сохранить
Применить
Сбросить

Рисунок 107. Обработка инцидентов

5.4.5 Фильтр содержимого

Страница **Фильтр содержимого** (см. Рисунок 108) 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 и инспекции UTM SSL (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 сервер, sql-сервер). Задается уровень эвристического анализа (см. [5.4.5.2 Настройки переменных фильтра содержимого](#)).

Настройка количества обслуживающих процессов

Активный (inline) режим	☒
Экземпляры	2
Пассивный режим	☒
Интерфейсы	eth1
Инспекция WAF	2
Инспекция UTM SSL	2

Настройки переменных фильтра содержимого

Внутренние сети	172.16.157.0/24,192.168.157.0/24
DNS-серверы	192.168.13.89,192.168.13.162,\$HOME_NET
Веб-серверы	172.16.157.10
SMTP-серверы	\$HOME_NET
Внешние сети	!\$HOME_NET
SQL-серверы	\$HOME_NET
Внешние сети WAF	!\$HTTP_SERVERS
Уровень эвристического анализа	Низкий

SSL-порты	443
HTTP-порты	80,81,8000:8900
SSH-порты	22
Порты передачи файлов	20
FTP-порты	21
SMTP-порты	25
Oracle-порты	66

Сохранить

Применить

Сбросить

Рисунок 108. Фильтр содержимого

5.4.5.1 Настройка количества обслуживающих процессов

Данный блок настроек включает следующие параметры (см. Рисунок 108):

- **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;



При использовании активного режима 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 использования 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 (параметр доступен при включенной инспекции WAF);
- **Инспекция UTM SSL.** Параметр позволяет выбрать количество процессов, которые будут использоваться в связке с прокси-сервером при инспекции UTM (параметр доступен при включенной инспекции UTM SSL).



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 108):

- **Внутренние сети.** Поле содержит IP-адреса защищаемых внутренних сетей и задает переменную \$HOME_NET;
- **DNS-серверы.** Поле содержит IP-адреса DNS-серверов в сети и задает переменную \$DNS_SERVERS. По умолчанию принимает значение \$HOME_NET;
- **Веб-серверы.** Поле содержит IP-адреса веб-серверов в сети и задает переменную \$HTTP_SERVERS. По умолчанию принимает значение IP-адреса защищаемого сервера;
- **SMTP-серверы.** Поле содержит IP-адреса почтовых серверов в 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, обнаружение ответов с состоянием «Filtered» не производится;
 - 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;

- **HTTP-порты.** Порты, на которые контекстный фильтр будет ожидать HTTP-трафик. По умолчанию принимает значение 80, 81, 8000:8900;
- **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 109) доступен просмотр и управление службами **WAF Dallas Lock**. Страница содержит следующие параметры:

- **Приоритет.** В столбце отображается текущий приоритет службы;
- **Скрипт инициализации.** В столбце отображается наименование службы;
- **Статус.** В столбце отображается текущий статус службы (Запущен или Остановлен);
- Столбец, где расположены кнопки **Включено** и **Отключено**, позволяющие включить или отключить автозапуск службы при загрузке **WAF Dallas Lock**;
- **Действия.** В столбце расположены кнопки **Старт**, **Перезапустить**, **Остановить**, позволяющие произвести соответствующие действия со службами.

Действия со службами, не влияющими на выполнение функций безопасности **WAF Dallas Lock** (odhcpd, keepalived, smartd, watchcat) не регистрируются в журналах, действия с остальными службами регистрируются в журнале *Системный*. Включение и отключение автозагрузки служб регистрируется в журнале *Политики*.



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

Скрипты инициализации ⓘ

Приоритет	Скрипт инициализации	Статус	Включено	Действия
12	dropbear	Остановлен	Включено	Старт Перезапустить Остановить
12	syslog-ng	Запущен	Включено	Старт Перезапустить Остановить
14	firewall	Запущен	Включено	Старт Перезапустить Остановить
15	network	Запущен	Включено	Старт Перезапустить Остановить
16	mosquitto	Запущен	Включено	Старт Перезапустить Остановить
19	dnsmasq	Запущен	Включено	Старт Перезапустить Остановить
24	octopus	Запущен	Включено	Старт Перезапустить Остановить
25	wafuacd	Остановлен	Включено	Старт Перезапустить Остановить
35	odhcpd	Запущен	Включено	Старт Перезапустить Остановить
50	cron	Запущен	Включено	Старт Перезапустить Остановить
50	uhttpd	Запущен	Включено	Старт Перезапустить Остановить
70	uproxy	Остановлен	Включено	Старт Перезапустить Остановить
70	wproxy	Запущен	Включено	Старт Перезапустить Остановить
71	keepalived	Остановлен	Включено	Старт Перезапустить Остановить
80	collectd	Запущен	Включено	Старт Перезапустить Остановить
90	ctf	Запущен	Включено	Старт Перезапустить Остановить
95	smartd	Запущен	Включено	Старт Перезапустить Остановить
97	watchcat	Остановлен	Включено	Старт Перезапустить Остановить
98	sysntpd	Запущен	Включено	Старт Перезапустить Остановить

Рисунок 109. Скрипты инициализации

Описание служб **WAF Dallas Lock** представлено ниже (см. Таблица 9).

Таблица 9. Список служб

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

5.4.7 Запланированные задания

Данная страница (см. Рисунок 110) позволяет администратору системы настроить расписание обновлений БРП, репутационных списков и данных GEO IP фильтра.

Задание */sbin/repdownload* позволяет запускать процедуру обновлений репутационных списков и данных GEO IP фильтра. Задание */sbin/rjdownload* позволяет запускать процедуру обновлений БРП COB и WAF.

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

Запланированные задания ⓘ

Час	Минута	Задание	Комментарий
05	35	/sbin/repdownload	Обновление репутационных списков
05	04	/sbin/rjdownload	Обновление БРП

Применить

Сбросить

Рисунок 110. Запланированные задания

5.4.8 Резервное копирование и перепрошивка

Данная страница (см. Рисунок 111) позволяет администратору создать архив текущих конфигурационных настроек **WAF Dallas Lock**, восстановить конфигурационные настройки из ранее

сохраненного архива.



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.

Настройки ^	Сеть v	Перезагрузка
WAF >		
UTM >		
Настройки модуля ECU		
Общие >	Система	
Пользователи >	Настройки интерфейса управления WAF DL	
Сервисы >	Параметры аудитора	
Управление сертификатами >	Фильтр содержимого	
Защита от Dos/DDos >	Управление службами	
Аварийный режим	Запланированные задания	
GEO IP фильтр	Резервное копирование / Перепрошивка	

Рисунок 111. Резервное копирование/Перепрошивка

Вкладка *Действия* (см. Рисунок 112). 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.

Действия

Прошивка/Сброс

Резервное копирование

Нажмите 'Создать архив', чтобы загрузить div-архив текущих config файлов прошивки устройства, таким образом вы сохраните его настройки. Для сброса настроек прошивки к исходному состоянию нажмите 'Выполнить сброс' (возможно только для squashfs-образов).

Создать архив

Восстановить резервную копию

Чтобы восстановить config файлы (ваши настройки прошивки устройства). Вы можете загрузить ранее созданный вами архив здесь. Устройство будет автоматически перезагружено.

Рисунок 112. Резервное копирование

Вкладка *Прошивка/Сброс* (см. Рисунок 113), блок **Установить новый образ прошивки**, позволяет заменить текущую прошивку на другую (требуется совместимый образ прошивки) либо переустановить действующую прошивку. Для этого необходимо нажать кнопку **Установить** и выбрать заранее сохраненный на устройство образ прошивки. Чекбокс *Сохранить настройки* может быть применен для того, чтобы сохранить текущие конфигурационные настройки системы.

Действия

Прошивка/Сброс

Установить новый образ прошивки

Загрузите suupgrade-совместимый образ, чтобы заменить текущую прошивку устройства. Поставьте галочку 'Сохранить настройки', чтобы сохранить текущие config файлы - ваши настройки устройства (требуется совместимый образ прошивки).

☒ **Сохранить настройки**

Рисунок 113. Образ прошивки



По вопросам совместимых версий прошивки следует обращаться в службу технической поддержки по электронному адресу: helpdesk@confident.ru.

Блок **Сброс к заводским настройкам** (см. Рисунок 114). 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**. При сбросе на заводские настройки доступ к веб-интерфейсу **WAF Dallas Lock** возможен только с компьютера, находящегося в локальной вычислительной сети. URL по умолчанию: <https://192.168.1.1:7443/>

Сброс к заводским настройкам

ВНИМАНИЕ! БУДЬТЕ ОСТОРОЖНЫ!

Нажатие кнопки "Сбросить" приведет к удалению всех заданных вами параметров и потребует полной перенастройки системы

Сбросить

Рисунок 114. Сброс к заводским настройкам

5.5 Настройка пользователей

Данная страница (см. Рисунок 115) позволяет создавать, удалять, изменять учетные записи пользователей, использующиеся для доступа к веб-интерфейсу **WAF Dallas Lock**.

Имя	Аутентификация	Разрешить квитиование ¹	
auditor	Без пароля	Нет	Изменить Удалить
user	По паролю	Нет	Изменить Удалить

Добавить +

Применить

Сбросить

Рисунок 115. 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 просмотр параметров системы. 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 116) кнопкой **Добавить**. В данной форме можно задать следующие параметры:

- имя пользователя (может содержать только строчные символы и цифры);
- 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 квитиование (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**.



Ошибка «Имя пользователя не разрешено к использованию» появляется при попытке создать учетную запись, имя которой уже используется в системе **WAF Dallas Lock**.

Рисунок 116. Форма добавления пользователя

Заблокированные пользователи

Для просмотра списка заблокированных учетных записей пользователей **WAF Dallas Lock** перейти на страницу **Настройки — Пользователи — Заблокированные пользователи** (см. Рисунок 117).

Настройки ^	Сеть v
WAF >	
UTM >	
Настройки модуля ЕЦУ >	
Общие >	
Пользователи >	Пользователи
Сервисы >	<u>Заблокированные пользователи</u>

Рисунок 117. 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 118). В таком случае у пользователя появляется возможность осуществить вход в систему снова.

Фильтр...

1 / 1

Пользователь ^	IP-адрес	Истекает	Удалить
unknow	192.168.131.81	1м 52с	Удалить

Рисунок 118. Список заблокированных пользователей

Для разблокирования конкретной учетной записи необходимо выбрать ее из списка

Заблокированные пользователи и нажать на кнопку **Удалить**.

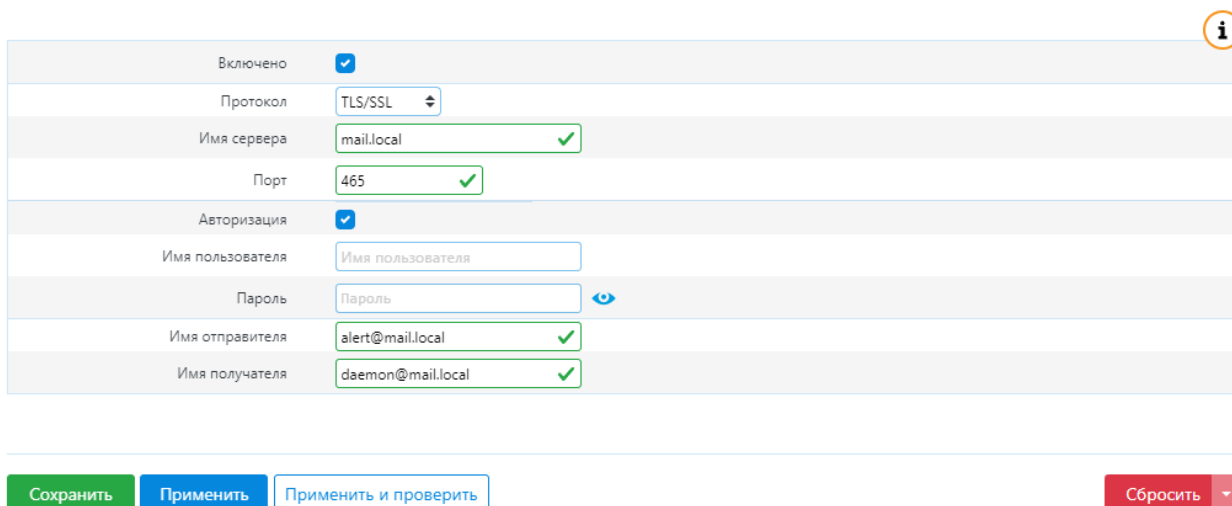
5.6 Настройка сервисов

5.6.1 Настройка почтовых уведомлений

WAF Dallas Lock позволяет настроить уведомление администратора об обнаруженных атаках по электронной почте (см. Рисунок 119).

- *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, откуда будет идти отправка уведомлений, нужно 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 уведомление и куда соответственно.

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



Включено	☒
Протокол	TLS/SSL
Имя сервера	mail.local ✓
Порт	465 ✓
Авторизация	☒
Имя пользователя	Имя пользователя
Пароль	Пароль
Имя отправителя	alert@mail.local ✓
Имя получателя	daemon@mail.local ✓

Сохранить Применить Применить и проверить Сбросить

Рисунок 119. Настройка почтовых уведомлений

5.6.2 Настройка сторожевого таймера

Сторожевой таймер позволяет настроить периодическую перезагрузку **WAF Dallas Lock** или перезагрузку при потере интернет-соединения на определенное администратором время (см. Рисунок 120).

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

Включено	☒
Режим работы	Перезагрузка при поте
Задержка принудительной перезагрузки	30
Период	6h
Хост пинг-запроса	8.8.8.8
Период пинг-запроса	30d

Сохранить Применить Сбросить

Рисунок 120. Настройка сторожевого таймера

5.7 Управление сертификатами

WAF Dallas Lock использует защищенный протокол HTTPS для управления устройством, может перехватывать и дешифровать 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 121) имеется список серверных сертификатов в системе для защищаемых узлов. В строке *Сгенерировать сертификат* можно создать самоподписанный 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**.

Серверные сертификаты Сертификаты УЦ Клиентские сертификаты

Сгенерировать сертификат

Имя ресурса [CN] 730 дней 2048 бит Сгенерировать

[Перейти к защищаемым ресурсам](#)

Список сертификатов

Имя ресурса [CN]	Истекает	Локальный	Отпечаток	Тип ключа	Действия
server.dl.local	01.04.2027	☒	33d7b940	RSA/2048	Посмотреть Изменить... Удалить

Сохранить Применить Сбросить

Рисунок 121. Список сертификатов



При окончании срока действия сертификата дата в столбце *Истекает* будет подсвечена красным.

Для того чтобы добавить сертификат стороннего УЦ необходимо нажать на ссылку *Перейти к защищаемым ресурсам* (см. Рисунок 122). 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.

Домены для инспекции Веб МЭ

Имя ресурса	Защищаемый сервер	Включено	HTTP	
server.dl.local	server.dl.local	☒	☒	Изменить Удалить

Загрузить новый сертификат

Добавить защищаемый ресурс

[Перейти к генерации сертификатов](#)

Рисунок 122. Добавление защищаемого узла и сертификата

5.7.2 Сертификаты УЦ

На данной вкладке (см. Рисунок 123) 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 [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;
- CA Client WAF DL промежуточный сертификат УЦ (intermediate CA) для создания самоподписанных клиентских сертификатов удаленного доступа.

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.

Серверные сертификаты

Сертификаты УЦ

Клиентские сертификаты

Настройки заголовков сертификатов

Расположение	Spb
Организация	AA Company Ltd
Подразделение	WAF

Локальные сертификаты

Общее имя [CN]	Истекает	Отпечаток	Тип ключа	Действия
CA Root WAF DL / ipsec	25.01.2035	b6cb9d10	RSA/4096	Посмотреть Скачать Изменить
CA VHost WAF DL	05.03.2030	a0888e67	RSA/4096	Посмотреть Скачать Изменить
CA UTM WAF DL	05.03.2030	499c3ef1	RSA/4096	Посмотреть Скачать Изменить
CA Client WAF DL	01.01.2030	e2b6b926	RSA/4096	Посмотреть Скачать Изменить

Дополнительные сертификаты

Общее имя [CN]	Истекает	Отпечаток	Тип ключа	Действия
- На данный момент список пуст -				

Добавить дополнительный сертификат:

...

Добавить

Сохранить

Применить

Сбросить

Рисунок 123. Локальные сертификаты

5.7.3 Клиентские сертификаты

На данной вкладке (см. Рисунок 124) имеется список клиентских сертификатов в системе для удаленного подключения. В строке *Сгенерировать сертификат удаленного доступа* можно создать самоподписанный сертификат для клиентов.

Для создания самоподписанного сертификата необходимо указать имя ресурса, ключ безопасности, количество дней действия сертификата, выбрать размер ключа и нажать кнопку **Сгенерировать**, после чего сертификат будет автоматически скачан в файловую систему ОС.

Кнопка **Посмотреть** служит для просмотра информации о сертификате.

Кнопка **Перевыпустить** служит для обновления срока действия сертификата, ключа безопасности или изменения длины ключа.

Кнопка **Отозвать** служит для отзыва клиентского сертификата, для подтверждения действия необходимо нажать кнопку **ОК** в открывшемся окне.

Серверные сертификаты
Сертификаты УЦ
Клиентские сертификаты

Сгенерировать сертификат удалённого доступа

✓
 ✓
 ✓
дней

Список сертификатов

Имя ресурса [CN]	Истекает	Отпечаток	Действия
test	31.03.2027	4eaf82b5	Посмотреть Перевыпустить Отозвать
test1000	01.04.2027	8172ba9d	Посмотреть Перевыпустить Отозвать

Рисунок 124. Клиентские сертификаты

5.8 Защита от DoS/DDoS атак

WAF Dallas Lock реализует защиту от DoS/DDoS атак на двух уровнях сетевой модели OSI:

- на прикладном уровне (уровне приложения) DoS/DDoS атаки направлены на нарушение доступности и корректной работы веб-приложений;
- на транспортном уровне (уровне протокола) DoS/DDoS атаки направлены на перегрузку каналов связи и нарушение работы протоколов TCP/UDP.

5.8.1 Прикладной уровень (WAF)

Вкладка *Прикладной уровень (WAF)* (см. Рисунок 125) содержит в себе два блока настроек, позволяющих установить параметры для снижения влияния DoS/DDoS атак на веб-приложение.

Блок настроек **Защита от сессионных атак** включает в себя следующие поля настроек:

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

Блок настроек **Защита от Flood-атак** представлена следующими настройками:

- *Максимальное число клиентов без client id.* Применяется для защиты от ботов. Задаёт ограничение количества клиентов без client id, отправляющих запросы с одного IP-адреса. Поле «за» задаёт временной интервал;
- *Включить ограничение числа запросов.* При активации чекбокса станут доступны следующие настройки HTTP запросов:
 - *Максимальное число запросов от одного клиента.* Задаёт ограничение числа запросов защищаемого ресурса от одного клиента. Применяется для защиты от атак scanning, HTTP-flood . Поле «за» задаёт временной интервал;
 - *Максимальное число запросов с ошибками.* Задаёт ограничение числа запросов с ошибками на защищаемом ресурсе . Поле «за» задаёт временной интервал.

Прикладной уровень (WAF)

Транспортный уровень

Защита от сессионных атак

Количество открытых соединений	32000	✓
Переход в усиленную защиту при достижении	80	✓ %

Тайм-аут HTTP запросов	5s	✓
Тайм-аут для клиента	5s	✓
Тайм-аут для HTTP туннелей	1h	✓

Защита от Flood-атак

Максимальное число клиентов без client id	15	✓
за	10s	✓
Включить ограничение числа запросов	☒	
Максимальное число запросов от одного клиента	50	✓
за	20s	✓
Максимальное число запросов с ошибками	25	✓
за	20m	✓

Сохранить

Применить

Сбросить

Рисунок 125. Защита от Dos/DDos. Прикладной уровень (WAF)

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.

5.8.2 Транспортный уровень

Вкладка *Транспортный уровень* позволяет установить параметры для снижения влияния DoS/DDoS атак на каналы связи и сетевые протоколы (см. Рисунок 126).

Блок общих настроек предусматривает параметры защиты от SYN-flood атак, использующих уязвимости при установке соединения по протоколу TCP. Для отслеживания и блокировки SYN-flood атак необходимо включить защиту нажав чекбокс *Включить защиту от SYN flood атак* и указать параметры:

- *Ограничение пакетов*. Задаёт предельное количество пропускаемых пакетов с флагом SYN за одну секунду.
- *Пиковый предел*. Задаёт максимальный размер буфера для пропуска пакетов с флагом SYN.

Параметр *Ограничение количества полуоткрытых соединений* ограничивает длину очереди полуоткрытых соединений (half-open connection). При превышении заданного значения последующие запросы на открытие TCP-соединений будут заблокированы.

Прикладной уровень (WAF)

Транспортный уровень

Включить защиту от SYN flood атак ⓘ ☒

Ограничение пакетов в секунду ✓

Пиковый предел ✓

Ограничение количества полукрытых соединений ⓘ ✓

Режим усиленной защиты от DoS/DDoS (L4) ⓘ

Переход в усиленную защиту при достижении ⓘ % ✓

Усиленная защита для протокола TCP ⓘ ☒

Ограничение трафика (TCP) ✓ Mb

Коэффициент пикового предела трафика (TCP) ✓

Пиковый предел трафика (TCP) Mb

Усиленная защита для протокола UDP ⓘ ☒

Ограничение трафика (UDP) ✓ Mb

Коэффициент пикового предела трафика (UDP) ✓

Пиковый предел трафика (UDP) Mb

Защита от DoS/DDoS сигнатурным методом ⓘ

Активизировать "DoS/DDoS" пресет: ⓘ [Добавить и перейти](#)

Нажмите "Применить" после перехода к странице пресетов!

Рисунок 126. Защита от Dos/DDoS. Транспортный уровень

Блок настроек **Режим усиленной защиты от DoS/DDoS (L4)** представлен следующими настройками:

- *Переход в усиленную защиту при достижении.* Параметр задает значение в процентах объем трафика относительно пропускной способности канала на интерфейсе WAN.
- *Усиленная защита для протокола TCP.* Чекбокс активирует/деактивирует ограничения трафика по протоколу TCP в режиме усиленной защиты и делает доступными для редактирования следующие параметры:
 - *Ограничение трафика (TCP).* Параметр задает предельное значение трафика в секунду по протоколу TCP в режиме усиленной защиты;
 - *Коэффициент пикового предела трафика (TCP).* Параметр задает предельное значение трафика по протоколу TCP в режиме усиленной защиты.
- *Усиленная защита для протокола UDP.* Чекбокс активирует/деактивирует ограничения трафика по протоколу UDP в режиме усиленной защиты и делает доступными для редактирования следующие параметры:
 - *Ограничение трафика (UPD).* Параметр задает предельное значение трафика в секунду по протоколу UDP в режиме усиленной защиты;
 - *Коэффициент пикового предела трафика (UDP).* Параметр задает предельное значение трафика по протоколу UDP в режиме усиленной защиты.



Перед переходом к настройке защиты от DoS/DDoS сигнатурным методом рекомендуется сохранить и применить изменения.

Блок настроек **Защита от DoS/DDoS сигнатурным методом** позволяет активировать функциональную возможность защиты от DoS/DDoS сигнатурным методом. Для активации параметра необходимо нажать кнопку **Добавить и перейти**, после чего произойдет переход на вкладку *Пресеты* фильтра содержимого UTM. На вкладке *Пресеты* необходимо активировать пресет «DoS/DDoS» последовательным нажатием кнопок **Сохранить** и **Применить** (более подробно в разделе [5.2.2 Фильтр содержимого](#)).

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.

5.9 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.

5.9.1 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 127). 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.

Кнопка **Очистить** предназначена для очистки всех журналов аудита. В открывшемся окне необходимо нажать кнопку **ОК** для выполнения очистки журналов.



При очистке журналов аудита **WAF Dallas Lock** перезагрузится для применения изменений.

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.

Аварийный режим **Активировать сейчас** ⓘ

Проверить систему ⓘ **Проверить**

Очистить все записи в журналах ⓘ **Очистить**

Использование дискового пространства ⓘ

Порог предупреждения (%) ⓘ	80 ✓
Порог аварийного режима (%) ⓘ	90 ✓

Сохранить **Применить** **Сбросить** ▾

Рисунок 127. Аварийный режим

5.9.2 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 очистки журналов или 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.

5.10 GEO IP фильтр

WAF Dallas Lock позволяет настроить доступ к защищаемому ресурсу из определенных стран по геолокации на основе IP-адреса (см. Рисунок 128):

- *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 следует нажать кнопку **Применить**.

Фильтр...

Сбросить

☐ Автоматически

Проверить обновления

Запретить трафик из стран 5

Страна	Континент	
Австралия	Австралия	Разрешить
Австрия	Европа	Разрешить
Азербайджан	Азия	Разрешить
Албания	Европа	Разрешить
Алжир	Африка	Разрешить

Разрешить все

Разрешить трафик из стран 188

Страна	Континент	
Ангола	Африка	Запретить
Андорра	Европа	Запретить
Антигуа и Барбуда	Северная Америка	Запретить
Аргентина	Южная Америка	Запретить
Армения	Азия	Запретить
Афганистан	Азия	Запретить
Багамские Острова	Северная Америка	Запретить

Запретить все

Применить

Рисунок 128. 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 129).

Данный раздел содержит следующие страницы:

- интерфейсы;
- DHCP и DNS;
- имена хостов;
- статические маршруты;
- межсетевой экран, содержит вкладки:
 - основные настройки;
 - перенаправление трафика;
 - правила для трафика;
 - правила аудита трафика;
 - списки доступа МЭ;
 - пользовательские правила;
- удаленный доступ, содержит вкладки:
 - основные настройки;
 - реквизиты для входа;
- качество обслуживания (QoS);
- диагностика.

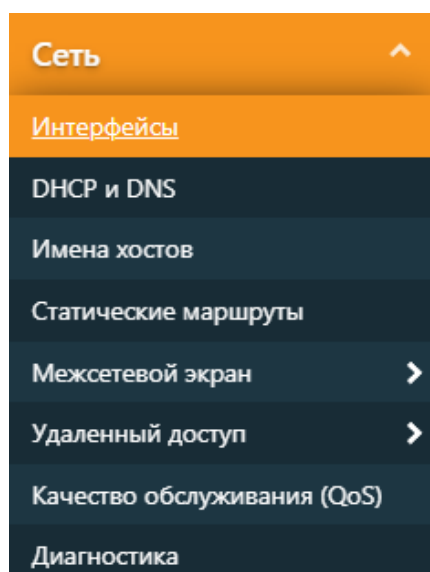


Рисунок 129. Сеть

6.1 Интерфейсы

На данной странице можно настроить сетевые интерфейсы LAN, IPv4 WAN, IPv6 WAN, DMZ (см. Рисунок 130).

LAN
WAN
WAN6
DMZ

Список интерфейсов

Сеть	Статус	Действия
LAN br-lan	Время работы: 0h 11m 10s MAC-адрес: 00:50:56:A2:5B:FE Физические интерфейсы: eth0 Получение (RX): 2.30 MB (15700 Пакетов) Передача (TX): 2.03 MB (5364 Пакетов) IPv4: 192.168.157.1/24 IPv6: fd1c1662:5ef8:1::1/64	Соединить Остановить Изменить Удалить
WAN eth1	Время работы: 0h 11m 10s MAC-адрес: 00:50:56:A2:5F:D8 Получение (RX): 4.61 MB (17049 Пакетов) Передача (TX): 4.09 MB (12585 Пакетов) IPv4: 10.10.100.254/22	Соединить Остановить Изменить Удалить
WAN6 eth1	MAC-адрес: 00:50:56:A2:5F:D8 Интерфейс не существует или пока не подключен.	Соединить Остановить Изменить Удалить
DMZ eth2	Время работы: 0h 11m 10s MAC-адрес: 00:50:56:A2:CD:74 Получение (RX): 556.35 KB (8379 Пакетов) Передача (TX): 2.55 KB (18 Пакетов) IPv4: 172.16.16.1/24 IPv6: fd1c1662:5ef8:1::1/64	Соединить Остановить Изменить Удалить

Добавить новый интерфейс

Основные настройки сети

IPv6 ULA-Prefix

Сохранить
Применить
Сбросить

Рисунок 130. Интерфейсы

Для добавления нового интерфейса необходимо нажать кнопку **Добавить новый интерфейс** и на открывшейся странице внести параметры: указать имя, выбрать протокол, выбрать физический интерфейс или при необходимости создать мост между несколькими физическими или виртуальными интерфейсами (см. Рисунок 131).

При создании интерфейса можно задать виртуальные VLAN-интерфейсы. Для этого в поле *Пользовательский интерфейс* необходимо ввести данные в формате «интерфейс.номер_VLAN», например eth0.1. Если необходимо назначить несколько VLAN одному интерфейсу, можно перечислить их через пробел, например: eth0.1 eth0.2.

Создать интерфейс

Имя нового интерфейса

Внимание: длина имени интерфейса

Протокол нового интерфейса
Статический адрес

Создать мост над несколькими интерфейсами
☒

Включить следующие интерфейсы

☒ Ethernet-адаптер: "eth0" (lan)
☒ Программное обеспечение VLAN: "eth0.1" (lan)
☐ Программное обеспечение VLAN: "eth0.2" (lan)
☐ Ethernet-адаптер: "eth1" (wan, wan6)
☐ Ethernet-адаптер: "eth2" (dmz)
☐ Пользовательский интерфейс:

Назад
Применить

Рисунок 131. Добавление нового интерфейса



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

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 132), 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.

LAN

WAN

WAN6

DMZ

Общие настройки

Дополнительные настройки

Настройки канала

Настройки межсетевого экрана

Состояние

br-lan

Время работы: 1h 28m 37s
MAC-адрес: 00:50:56:A2:86:33
Получение (RX): 4.40 MB (29986 Пакетов)
Передача (TX): 4.39 MB (11889 Пакетов)
IPv4: 192.168.157.1/24
IPv6: fd0c:f46e:fb15:1::1/64

Протокол

Статический адрес

IPv4-адрес

192.168.157.1

Маска сети IPv4

255.255.255.0

IPv4-адрес шлюза

Использовать метрику шлюза

0

Широковещательный IPv4-адрес

Использовать собственные DNS-серверы

Автоматическое назначение ULA адреса

64

IPv6 подсказка присвоения

IPv6 суффикс

::1

DHCP-сервер

Основные настройки

IPv6 Настройки

Игнорировать интерфейс

Назад

Сохранить

Применить

Сбросить

Рисунок 132. LAN — Основные настройки

Во вкладке для интерфейса LAN, в категории *Дополнительные настройки* (см. Рисунок 133), можно настроить параметры:

LAN

WAN

WAN6

DMZ

Общие настройки

Основные настройки

Дополнительные настройки

Настройки канала

Настройки межсетевого экрана

Запустить при загрузке	☒
Доверенный интерфейс	☒
Использовать встроенный IPv6-менеджмент	☒
Назначить MAC-адрес	00:50:56:A2:86:33
Назначить MTU	1500 ☒

DHCP-сервер

Основные настройки

IPv6 Настройки

Игнорировать интерфейс

☒

Назад

Сохранить

Применить

Сбросить

Рисунок 133. LAN — Дополнительные 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.
- *Доверенный интерфейс* (создание виртуального интерфейса для репликаций в кластере доступно только для доверенных интерфейсов). По умолчанию включен только для интерфейса LAN.
- *Использовать встроенный IPv6-менеджмент* (использование сервиса IP-management — IPAM). Для указанных настроек активация произойдет после проставления отметки напротив названия.
- *Назначить MAC-адрес* (позволяет подменить MAC-адрес интерфейса), по умолчанию принимает значение MAC-адреса интерфейса.
- *Назначить MTU* (максимальный размер полезного блока данных одного пакета).
- *Использовать шлюз по умолчанию* (использование шлюза, предоставляемого DHCP-сервером).
- *Шлюз по умолчанию* (использование шлюза, предоставляемого DHCP-сервером).
- *Использовать широковещательный флаг* (широковещательный бит при обращении к DHCP серверу), по умолчанию выключено.
- *Использовать метрику шлюза* (метрика интерфейса определяет затраты, связанные с использованием этого маршрута).
- *Использовать TTL на интерфейсе туннеля* (предельный период времени, число итераций или переходов, за который набор данных (пакет) может существовать до своего исчезновения на интерфейсе туннеля).
- *Использовать MTU на интерфейсе туннеля* (максимальный размер пакета данных для его передачи на интерфейсе туннеля).
- *Использовать объявляемые узлом DNS-серверы* (использование DNS-серверов, предоставляемых DHCP-сервером).

- *Использовать собственные DNS-серверы* (поля позволяют задать IP-адреса DNS-серверов для интерфейса), параметр доступен если отключен чекбокс *Использовать объявляемые узлом DNS серверы*.
- *Установленный IPv6-prefix* (часть адреса в протоколе IPv6, которая определяет принадлежность адреса к определенной подсети).
- *ID клиента при DHCP-запросе* (уникальный идентификатор устройства в сети при подключении к серверу DHCP).
- *Класс производителя (Vendor class)*, который отправлять при DHCP-запросах (идентификатор класса производителя для устройства позволяет DHCP-серверу определить тип устройства и предоставить соответствующий IP-адрес и параметры конфигурации).



Параметры могут отличаться для различных режимов работы интерфейсов (способа получения адреса интерфейса).

На вкладке для интерфейса LAN, в категории *Настройки канала* (см. Рисунок 134), можно выбрать настройки объединения в мост для указанных интерфейсов и назначить им виртуальные интерфейсы VLAN. 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).



При настройке интерфейса можно задать виртуальные VLAN-интерфейсы. Для этого в поле *Пользовательский интерфейс* необходимо ввести данные в формате «интерфейс.номер_VLAN», например eth0.1. Если необходимо назначить несколько VLAN одному интерфейсу, можно перечислить их через пробел, например: eth0.1 eth0.2.

Общие настройки

[Основные настройки](#)
[Дополнительные настройки](#)
[Настройки канала](#)
[Настройки межсетевого экрана](#)

Объединить в мост ☒

Включить STP ☐

Интерфейс

☒	Ethernet-адаптер: "eth0" (lan)
☒	Программное обеспечение VLAN: "eth0.1" (lan)
☒	Программное обеспечение VLAN: "eth0.2" (lan)
☐	Ethernet-адаптер: "eth1" (wan, wan6)
☐	Ethernet-адаптер: "eth2" (dmz)
☐	Пользовательский интерфейс:

DHCP-сервер

[Основные настройки](#)
[IPv6 Настройки](#)

Игнорировать интерфейс ☒

[Назад](#)
[Сохранить](#)
[Применить](#)
[Сбросить](#)

Рисунок 134. LAN — Настройки канала

На вкладке для интерфейса LAN, в категории *Настройки межсетевого экрана* (см. Рисунок 135), 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.

LAN WAN WAN6 DMZ

Общие настройки

Основные настройки | Дополнительные настройки | Настройки канала | Настройки межсетевого экрана

Создать / назначить зону сетевого экрана

☐

dmz: dmz:

☒

lan: lan:

☐

wan: wan: wan6: wan6:☐

DHCP-сервер

Основные настройки | IPv6 Настройки

Игнорировать интерфейс

Назад Сохранить Применить Сбросить

Рисунок 135. 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 136), 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.

LAN WAN WAN6 DMZ 123

Общие настройки

Основные настройки | Дополнительные настройки | Настройки канала | Настройки межсетевого экрана

Статус

eth1

Время работы: 17d 7h 11m 12s

MAC-адрес: 00:50:56:A2:C2:78

Получение (RX): 533.81 MB (8602542 Пакетов)

Передача (TX): 48.45 MB (132658 Пакетов)

IPv4: 10.10.101.141/22

Протокол: DHCP-клиент

Имя хоста в DHCP-запросах: WAF-2.16.20

Назад Сохранить Применить Сбросить

Рисунок 136. WAN — Основные настройки

На вкладке для интерфейса WAN6 (IPv6 WAN), в категории *Основные настройки* (см. Рисунок 137), можно увидеть текущее состояние интерфейса, а также указать основные настройки для интерфейса.

LAN WAN **WAN6** DMZ 123

Общие настройки

Основные настройки | Дополнительные настройки | Настройки канала | Настройки межсетевого экрана

Статус	eth1	MAC-адрес: 00:50:56:A2:C2:78 Интерфейс не существует или пока не подключен.
Протокол	DHCPv6 клиент	
Запрос IPv6 адреса	try	
Запрос IPv6 префикс длины	Автоматически	

Назад Сохранить Применить Сбросить

Рисунок 137. WAN6 — Основные настройки

На вкладке для интерфейса DMZ (*Demilitarized Zone*), в категории *Основные настройки* (см. Рисунок 138), можно увидеть текущее состояние интерфейса, а также указать основные настройки для интерфейса.

LAN WAN WAN6 **DMZ** 123

Общие настройки

Основные настройки | Дополнительные настройки | Настройки канала | Настройки межсетевого экрана

Статус	eth2	Время работы: 17d 7h 13m 2s MAC-адрес: 00:50:56:A2:6A:D4 Получение (RX): 766.49 MB (12066626 Пакетов) Передача (TX): 2.07 MB (12177 Пакетов) IPv4: 172.16.16.1/24 IPv6: fd00:a724:17fc:1/64
Протокол	Статический адрес	
IPv4-адрес	172.16.16.1 ✓	
Маска сети IPv4	255.255.255.0 ✓	
IPv4-адрес шлюза		
Использовать метрику шлюза	0	
Широковещательный IPv4-адрес		
Использовать собственные DNS-серверы	✗ +	
Автоматическое назначение ULA адреса	64 ✓	
IPv6 подкачка присвоения		
IPv6 суффикс	-1	

ДHCP-сервер

Основные настройки | IPv6 Настройки

Игнорировать интерфейс ☒

Назад Сохранить Применить Сбросить

Рисунок 138. 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.

DHCP-сервер

Дополнительные настройки	
Игнорировать интерфейс	☐
Старт	100 ✓
Предел	150 ✓
Время аренды адреса	12h

Назад Сохранить Применить Сбросить

Рисунок 139. DHCP-сервер — Основные настройки

На вкладке *Дополнительные настройки* (см. Рисунок 140) можно включить протокол динамической настройки узла, позволяющий устройствам автоматически получать IP-адреса.

DHCP-сервер

Дополнительные настройки	
Динамический DHCP	☒
Назначить	☐
IPv4-Маска сети	
DHCP-Настройки	

Назад Сохранить Применить Сбросить

Рисунок 140. DHCP-сервер — Дополнительные настройки

На вкладке *IPv6 настройки* (см. Рисунок 141) 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.

DHCP-сервер

IPv6 Настройки	
Доступные режимы работы	отключено
DHCPv6-Сервис	отключено
NDP-прокси	отключено
Объявить DNS-серверы	
Объявить DNS-домены	

Назад Сохранить Применить Сбросить

Рисунок 141. 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 142) можно указать основные настройки DHCP-сервера и DNS-прокси, содержащие следующие поля настроек:

- *Требуется домен.* При включенном чекбоксе DNS-запросы не будут перенаправляться без DNS-имени;
- *Авторизованный.* 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;



Поле для перенаправления DNS-запросов должно быть заполнено для корректной работы **WAF Dallas Lock**.

- **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*).

Настройки сервера



Основные настройки	Дополнительные настройки
Требуется домен	☒
Авторизованный	☐
Локальный сервер	/lan/
Локальный домен	lan
Запись запросов	☐
Перенаправление запросов DNS	/example.org/10.1.2.3
Защита от DNS Rebinding	☒
Разрешить локальный хост	☒
Белый список доменов	ucc.local
Только локальный DNS	☒
Не использовать wildcard	☒
Интерфейс для входящих соединений	
Исключите интерфейсы	

Рисунок 142. Основные настройки

Активные DHCP аренды, Активные DHCPv6 аренды (см. Рисунок 143) позволяют просматривать состояние активных арендованных адресов. Таблица **Постоянные аренды** (см. Рисунок 143) используется для присвоения DHCP-клиентам фиксированных IP-адресов и имен. Это необходимо для статических интерфейсов, в которых обслуживаются только клиенты с присвоенными IP-адресами.

Активные DHCP аренды

Имя хоста	IPv4-адрес	MAC-адрес	Оставшееся время аренды
Нет активных арендованных адресов.			

Активные DHCPv6 аренды

Хост	IPv6-адрес	DUID	Оставшееся время аренды
Нет активных арендованных адресов.			

Постоянные аренды ⓘ

Имя хоста	MAC-Адрес	IPv4-Адрес	Время аренды адреса	IPv6-Суффикс (hex)	
Client1	00:50:56:a2:a9:17 (15)	192.168.157.101	10m		Удалить

Добавить +

Рисунок 143. 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» — MAC-адрес хоста;
 - «IPv4-Адрес» — IP-адрес хоста;
 - «Время аренды адреса» время подключения (используются суффиксы «s» — для указания секунд, «m» — минут, «h» — часов, «d» — дней);
 - «IPv6-Суффикс (hex)» (см. Рисунок 144).



В данном разделе настроек (см. Рисунок 144) 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.

Постоянные аренды ⓘ

Имя хоста	MAC-Адрес	IPv4-Адрес	Время аренды адреса	IPv6-Суффикс (hex)	
Client1	00:50:56:a2:a9:17 (15)	192.168.157.101	10m		Удалить

Добавить +

Рисунок 144. Добавление постоянной аренды

На вкладке *Дополнительные настройки* (см. Рисунок 145) 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.* Локализовать 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.

Настройки сервера



Основные настройки	Дополнительные настройки
Подавить логирование	☐
IP последовательно	☐
Фильтровать частные	☒
Фильтровать бесполезные	☐
Локализовывать запросы	☒
Расширять имена узлов	☒
Отключить кэш отрицательных ответов	☐
Дополнительные файлы серверов	
Строгий порядок	☐
Переопределение поддельного NX-домена	67.215.65.132 [-] [+]
DNS порт сервера	53
DNS порт запроса	любой
Макс. кол-во аренд DHCP аренды	неограниченный
Макс.EDNS0 размер пакета	1232 ✓
Макс. кол-во одновременных запросов	150

Рисунок 145. Дополнительные настройки



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 **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.

6.3 Имена хостов

Данная страница (см. Рисунок 146) 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.

DMZ	Имя хоста	IP-адрес
☒	node1_1 ✓	172.16.157.10 (00:50) ✓ Удалить

Добавить +

Сохранить Применить Сбросить ▾

Рисунок 146. Имена хостов

6.4 Статистические маршруты

На данной странице (см. Рисунок 147) 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 **Удалить** позволяет удалить выбранный статический маршрут.

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.

Статические маршруты IPv4 ⓘ

Интерфейс	Адрес назначения ⓘ	Маска сети ⓘ	Шлюз	Метрика	MTU	Тип маршрута
lan ▾	192.168.157.10	255.255.255.0	192.168.157.1	0	1500	unicast ▾ Удалить

Добавить +

Статические маршруты IPv6

Интерфейс	Адрес назначения ⓘ	Шлюз	Метрика	MTU	Тип маршрута
- На данный момент список пуст -					

Добавить +

Сохранить Применить Сбросить ▾

Рисунок 147. Статические маршруты

6.5 Межсетевой экран

На странице **Межсетевой экран** можно создать и настроить зоны сети для контроля трафика. Страница (см. Рисунок 148) содержит следующие вкладки:

- основные настройки;
- перенаправление портов;
- правила для трафика;
- правила аудита трафика;
- списки доступа МЭ;
- 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 148) 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*.

Параметр *Ограничить журнал сообщений* позволяет настроить количество журналируемых МЭ событий за определенный период.



При заполнении поля *Ограничить журнал сообщений* необходимо задать параметр следующего вида «число запросов/период времени». Для указания периода времени используются следующие сокращения: «s (second)» — для указания секунд, «m (minute)» — минут, «h (hour)» — часов, «d (day)» — дней.

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 маскардинга и ограничения MSS. Для каждого правила присутствуют отдельные кнопки **Изменить/Удалить**.

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

Основные настройки

Не пропускать некорректные пакеты ☐

Ограничить журнал сообщений 10/minute ✓

Входящий трафик: принимать

Исходящий трафик: принимать

Перенаправление: отвергать

Зоны

Зона → Перенаправления	Входящий трафик	Исходящий трафик	Перенаправление	Маскардинг	Ограничение MSS	Изменить	Удалить
lan: lan → wan: dmz	принимать	принимать	принимать	☐	☐	Изменить	Удалить
wan: wan → wan: dmz	отвергать	принимать	отвергать	☒	☒	Изменить	Удалить
dmz: dmz → wan	принимать	принимать	отвергать	☐	☐	Изменить	Удалить

Добавить +

Сохранить Применить Сбросить

Рисунок 148. Основные настройки

6.5.2 Перенаправление портов

На вкладке можно настроить перенаправление (проброс) портов (см. Рисунок 149). 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.

В списке **Перенаправление портов** есть возможность включать/отключать и сортировать правила. Для каждого правила присутствуют отдельные кнопки **Изменить** и **Удалить**. При нажатии кнопки **Изменить** откроется страница для редактирования параметров перенаправления портов.

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**, отобразится страница изменения параметров нового правила перенаправления, после настройки параметров необходимо нажать кнопку **Применить**.

The screenshot shows the 'Перенаправление портов' (Port Forwarding) section of the WAF Dallas Lock configuration interface. At the top, there are tabs for 'Основные настройки', 'Перенаправление портов', 'Правила для трафика', 'Правила аудита трафика', 'Списки доступа МЭ', and 'Пользовательские правила'. Below the tabs, there is a table of existing rules. The table has columns: 'Имя', 'Перенаправить из', 'Перенаправить в', 'Включить', and 'Сортировка'. One rule is listed: 'WAF- HTTP' with 'IPv4 TCP' as the source, 'IP 192.168.1.10, порт 80 в dmz' as the destination, and the 'Включить' checkbox is unchecked. Below the table, there is a section 'Новое перенаправление порта:' with a form to add a new rule. The form has fields for 'Имя', 'Протокол' (set to TCP+UDP), 'Внешняя зона' (set to dmz), 'Внешний порт', 'Внутренняя зона' (set to dmz), 'Внутренний IP-адрес', and 'Внутренний порт'. There is a 'Добавить' button next to the form. At the bottom of the page, there are buttons for 'Сохранить', 'Применить', and 'Сбросить'.

Рисунок 149. Перенаправление портов

На странице редактирования параметров правил перенаправления портов (см. Рисунок 150), доступны следующие параметры:

- *Правило включено/правило выключено* — параметр позволяет управлять включением/отключением правила перенаправления портов;
- *Имя* — параметр позволяет задать имя правила;
- *Протокол* — параметр позволяет выбрать из раскрывающегося списка протокол, который будет использоваться для передачи данных;
- *Зона источника* — параметр позволяет выбрать из списка зону внешней сети;
- *MAC-адрес источника* — параметр позволяет установить MAC-адрес источника, для которого применяется правило;
- *IP-адрес источника* — параметр позволяет установить IP-адрес источника, для которого применяется правило или указать что правило применяется для любого адреса;
- *Порт источника* — параметр позволяет указать порт, трафик с которого будет переадресовываться на IP-адрес, определяемый в поле *Внутренний IP-адрес*;
- *Внешний IP-адрес* — параметр позволяет указать внешний IP-адрес, который будет принимать трафик, определяемый в поле *Внутренний IP-адрес*;
- *Внешний порт* — параметр позволяет указать порт, на который будет переадресовываться трафик с порта, задаваемого в поле *Внутренний порт*;
- *Внутренняя зона* — параметр позволяет выбрать зону внутренней сети. Выбрать необходимое значение из раскрывающегося списка;
- *Внутренний IP-адрес* — параметр позволяет 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 --»;
- *Внутренний порт* — параметр позволяет указать порт, на который будет переадресовываться трафик с порта, задаваемого в поле *Внешний порт*;
- *Включить NAT Loopback* — чекбокс позволяет управлять политикой применения технологией NAT Loopback для правила перенаправления трафика;
- *Дополнительные аргументы* — параметр позволяет указать дополнительные аргументы iptables для правила.

Межсетевой экран - Перенаправление портов - WAF-HTTP ⓘ

Правило выключено	Включить
Имя	WAF-HTTP
Протокол	TCP
Зона источника	☐ dmz: dmz: ⓘ ☐ lan: lan: ⓘ ☒ wan: wan: ⓘ wan6: wan6: ⓘ
MAC-адрес источника ⓘ	-
IP-адрес источника ⓘ	любой
Порт источника ⓘ	любой
Внешний IP-адрес ⓘ	любой
Внешний порт ⓘ	80 ✓
Внутренняя зона	☒ dmz: dmz: ⓘ ☐ lan: lan: ⓘ ☐ wan: wan: ⓘ wan6: wan6: ⓘ
Внутренний IP-адрес ⓘ	192.168.1.10 ✓
Внутренний порт ⓘ	80 ✓
Включить NAT Loopback	☒
Дополнительные аргументы ⓘ	

Назад	Сохранить	Применить	Сбросить ▼
-------	-----------	-----------	------------

Рисунок 150. Параметры правила перенаправления портов.

6.5.3 Правила для трафика

На данной вкладке можно настроить правила для трафика (см. Рисунок 151), 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 добавить новое правило и отредактировать его.

Пункт **Правила для SNAT** отображает список созданных NAT-источников. Таблица позволяет визуально наблюдать список источников, а также сортировать и включать/отключать их. Для каждого правила присутствуют отдельные кнопки **Изменить/Удалить**.

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

Основные настройки Перенаправление портов Правила для трафика Правила аудита трафика Списки доступа МЭ Пользовательские правила ⓘ

Правила для трафика

Имя	Перенаправлять из	Действие	Включить	Сортировка	
Allow-DHCP-Renew	IPv4-UDP Из любого хоста в wan К.любой IP-адрес МЭ, порт порт 68 на этом устройстве	Импортировать	☒	↑ ↓	Изменить Удалить
Allow-Ping	IPv4-ICMP с тип echo-request Из любого хоста в wan К.любой IP-адрес МЭ на этом устройстве	Импортировать	☒	↑ ↓	Изменить Удалить
Allow-ICMPv6-Input	IPv6-ICMP Из любого хоста в wan К.любой IP-адрес МЭ на этом устройстве	Импортировать с пределом в 1000 пакетов за секунду	☒	↑ ↓	Изменить Удалить

Открыть порты на МЭ:

Имя	Протокол	Внешний порт	
Новое правило для входящего...	TCP+UDP		Добавить

Новое правило перенаправления:

Имя	Зона источника	Зона назначения	
Новое правило перенап...	lan	wan	Добавить и редактировать...

Правила для SNAT ⓘ

Имя	Перенаправлять из	Действие	Включить	Сортировка
- На данный момент список пуст -				

Новое правило для SNAT:

Имя	Зона источника	Зона назначения	К IP-адресу источника	К порту источника	
Новое правило SNAT	lan	wan	Не перезаписывать	Не перезаписывать	Добавить и редактировать...

Сохранить Применить Сбросить

Рисунок 151. Правила для трафика

Страница редактирования правила для трафика (см. Рисунок 152) позволяет настроить следующие параметры:

- *Правило включено/правило выключено* — параметр позволяет управлять включением/отключением правила для трафика;
- *Имя* — параметр позволяет задать имя правила;
- *Ограничить версию IP* — позволяет выбрать какая версия протокола IP необходима для правила;
- *Протокол* — параметр позволяет выбрать из раскрывающегося списка протокол, который будет использоваться для передачи данных;
- *Зона источника* — параметр позволяет выбрать зону источника из списка;
- *MAC-адрес источника* — параметр позволяет установить MAC-адрес источника, для которого применяется правило;
- *Адрес источника* — параметр позволяет установить IP-адрес источника, для которого применяется правило или указать что правило применяется для любого адреса;
- *Порт источника* — параметр позволяет указать порт, трафик с которого будет переадресовываться на IP-адрес, определяемый в поле *Адрес назначения*;
- *Зона назначения* — параметр позволяет выбрать зону внутренней сети из списка;
- *Адрес назначения* — параметр позволяет 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 --»;
- *Порт назначения* — параметр позволяет указать порт, на который будет переадресовываться трафик с порта, задаваемого в поле *Порт источника*;
- *Действие* — параметр позволяет настроить действие для трафика;

- *Дополнительные аргументы* — параметр позволяет указать дополнительные аргументы iptables для правила;
- *Дни недели, Дни месяца, Время начала, Время остановки, Дата начала, Дата остановки* — параметры позволяют управлять расписанием работы правила для трафика;
- *Время UTC* — чекбокс позволяет использовать время UTC, если параметр активирован или локальное, если параметр не активен.

Правила для трафика - test ⓘ

Правило включено	☒ Отключить
Имя	test
Ограничить версию IP	IPv4 и IPv6
Протокол	TCP+UDP
Зона источника	☐ Любая зона ☐ dmz: dmz: ☒ lan: lan: ☐ wan: wan: wanb:
MAC-адрес источника	любой
Порт источника	любой
Зона назначения	☐ Устройство (ввод) ☐ Любая зона (перенаправить) ☐ dmz: dmz: ☐ lan: lan: ☒ wan: wan: wanb:
Адрес назначения	любой
Порт назначения	любой
Действие	принимать
Дополнительные аргументы ⓘ	
Дни недели	☐ Понедельник ☐ Вторник ☐ Среда ☐ Четверг ☐ Пятница ☐ Суббота ☐ Воскресенье
Дни Месяца	☐ ВСЕ ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23 ☐ 24 ☐ 25 ☐ 26 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31
Время начала	...
Время остановки	...
Дата начала	дд.мм.гггг
Дата остановки	дд.мм.гггг
Время UTC	☐

Рисунок 152. Параметры правила для трафика

6.5.4 Правила аудита трафика

На данной вкладке можно настроить правила аудита трафика (см. Рисунок 153), 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. Для каждого правила присутствуют отдельные кнопки **Изменить/Удалить**.

Предустановленные правила позволяют настроить аудит трафика по протоколам SMTP, SMTPS, STARTTLS, IMAP, IMAPS, POP3, POP3S, RFB/VNC, AMQPS, XMPP с источником в зоне WAN, а также для портов HTTP, HTTPS и порта управления межсетевым экраном из любой зоны.

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 добавить новое правило и отредактировать его параметры.

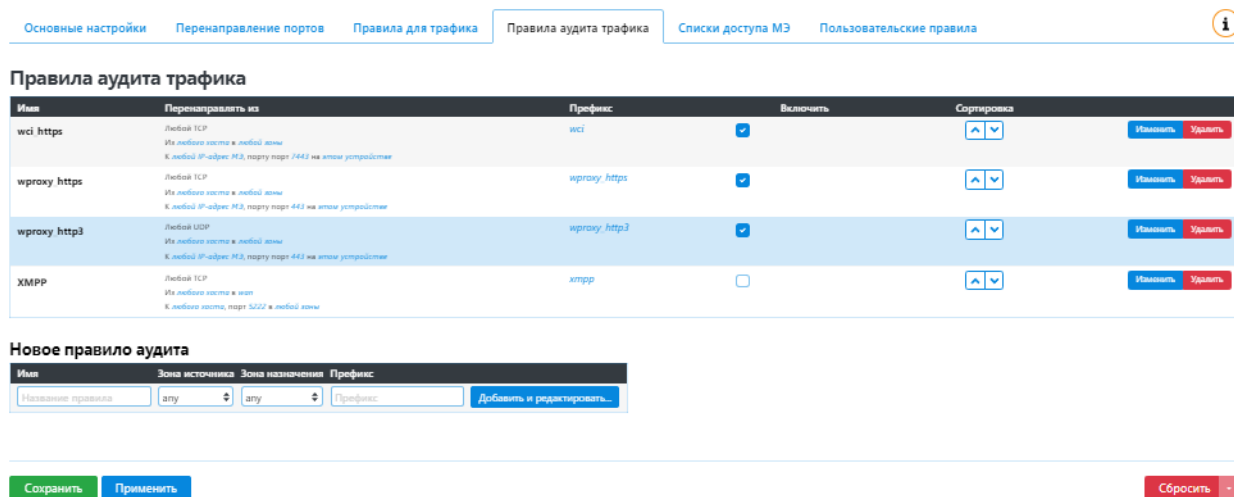


Рисунок 153. Правила аудита трафика

Страница редактирования правила для трафика (см. Рисунок 154) позволяет настроить следующие параметры:

Правила аудита трафика - test ⓘ

The screenshot shows the configuration page for a specific traffic audit rule named 'test'. The settings are as follows:

- Правило включено** (Rule enabled): ☒ (Отключить button)
- Имя** (Name): test
- Префикс** (Prefix): -
- Уровень логирования** (Logging level): warning (Внимание)
- Ограничить версию IP** (Limit IP version): IPv4 и IPv6
- Протокол** (Protocol): TCP+UDP
- Зона источника** (Source zone): Любая зона (selected), dmz: dmz, lan: lan, wan: wan, wan6: wan6
- MAC-адрес источника** (Source MAC address): любой
- Порт источника** (Source port): любой
- Зона назначения** (Destination zone): Любая зона (перенаправить) (selected), dmz: dmz, lan: lan, wan: wan, wan6: wan6
- Порт назначения** (Destination port): любой

At the bottom, there are buttons for 'Назад' (Back), 'Сохранить' (Save), 'Применить' (Apply), and 'Сбросить' (Reset).

Рисунок 154. Параметры правила аудита трафика

- *Правило включено/правило выключено* — параметр позволяет управлять включением/отключением правила аудита трафика;
- *Имя* — параметр позволяет задать имя правила;
- *Префикс* — параметр позволяет задать префикс;
- *Уровень логирования* — параметр позволяет задать уровень логирования для правила;

- *Ограничить версию IP* — позволяет выбрать какая версия протокола IP необходима для правила;
- *Протокол* — параметр позволяет выбрать из раскрывающегося списка протокол, который будет использоваться для передачи данных;
- *Зона источника* — параметр позволяет выбрать зону источника из списка;
- *MAC-адрес источника* — параметр позволяет установить MAC-адрес источника для которого применяется правило;
- *Адрес источника* — параметр позволяет установить IP-адрес источника для которого применяется правило или указать, что правило применяется для любого адреса;
- *Порт источника* — параметр позволяет указать порт, трафик с которого будет переадресовываться на IP-адрес, определяемый в поле *Адрес назначения*;
- *Зона назначения* — параметр позволяет выбрать зону внутренней сети из списка;
- *Адрес назначения* — параметр позволяет указать IP-адрес устройства, находящегося в локальной сети;
- *Порт назначения* — параметр позволяет указать порт, на который будет переадресовываться трафик с порта, задаваемого в поле *Порт источник*.

6.5.5 Списки доступа МЭ

На данной вкладке настраиваются списки доступа 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.

Списки доступа МЭ

Таймаут 3600 сек

Фильтр...

Разрешенные узлы 2

Хост	Таймаут	
192.168.157.2	11ч 15м 34с	Постоянная аренда Удалить
192.168.131.81	10ч 8м 47с	Постоянная аренда Удалить

Разрешенные сети

Хост	Таймаут
- На данный момент список пуст -	

Разрешенные IPv6 узлы

Хост	Таймаут
- На данный момент список пуст -	

Разрешенные IPv6 сети

Хост	Таймаут
- На данный момент список пуст -	

Запрещенные узлы

Хост	Таймаут
- На данный момент список пуст -	

Запрещенные сети

Хост	Таймаут
- На данный момент список пуст -	

Запрещенные IPv6 узлы

Хост	Таймаут
- На данный момент список пуст -	

Запрещенные IPv6 сети

Хост	Таймаут
- На данный момент список пуст -	

Рисунок 155. Списки доступа МЭ

В таблицах (см. Рисунок 155) **Разрешенные узлы**, **Разрешенные сети**, **Разрешенные IPv6 узлы**, **Разрешенные IPv6 сети** отображается информация о добавленных пользователем соединениях. В столбцах *Хост* отображаются подключенные IP-адреса. В столбцах *Таймаут* — оставшееся время подключения или блокировки IP-адресов в системе **WAF Dallas Lock**.

В данном разделе настроек (см. Рисунок 155) 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.

Блок управляющих кнопок (см. Рисунок 156):

- **Фильтр.** Сортирует значения в таблицах исходя из введенных данных в поле *Фильтр*;
- **Добавить.** По кнопке появляется всплывающее 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 156).

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

Списки доступа МЭ

Рисунок 156. Управляющие кнопки

Для добавления нового соединения в таблицы требуется выполнить следующие действия:

1. Нажать кнопку **Добавить**;
2. Во всплывающем окне *Добавление нового IP* (см. Рисунок 157) 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** в окне *Добавление нового IP* (кнопка **Заккрыть** отменяет действие, изменения не сохраняются).

Рисунок 157. Добавление нового IP

В **Списках доступа МЭ** реализована возможность загружать пользовательские списки и взаимодействовать с ними (см. Рисунок 159). 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 158);

TXT содержит IP адреса на каждой строчке 1 адрес. Или адрес или адрес сети. Пример:

```
192.168.1.1
10.10.10.200
10.10.11.252
192.168.3.0/24
```

CSV файл. Также содержит IP адрес или адрес сети, но разделенные ','.

```
192.168.1.1,10.10.10.200,10.10.11.252,192.168.3.0/24
```

Рисунок 158. Пример файла с IP-адресами

- **Обновить.** Кнопка отвечает за обновление списков в системе, избавляя от необходимости вручную удалять уже имеющийся список и загружать его новую версию;
- **Обновление по расписанию.** Чекбокс позволяет обновлять внесенные списки через заданный временной интервал (подробнее в разделе 5.4.7 Запланированные задания);
- **Удалить.** Кнопка удаляет выбранный список/списки.

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

Пункты **Список запрещенных узлов** и **Список разрешенных узлов** отображают наименования загруженных списков, состояние работы списков и позволяет управлять политикой регистрации событий при взаимодействии с IP-адресами или сетями из списков.

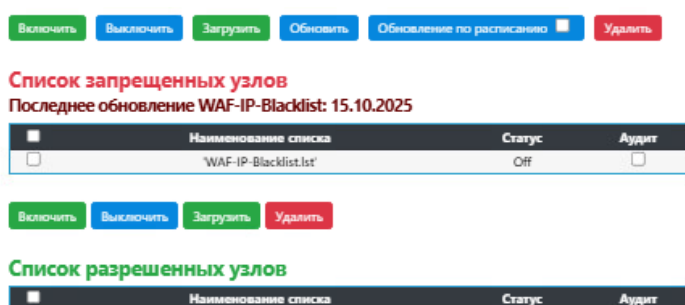


Рисунок 159. Загрузка списков

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 160). 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.

[Основные настройки](#)
[Перенаправление портов](#)
[Правила для трафика](#)
[Правила аудита трафика](#)
[Списки доступа МЭ](#)
[Пользовательские правила](#)

```

# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.

# using only 'iptables' 'ip6tables' 'ipset' with first position
# example:

iptables -A input_log -p tcp -m tcp --dport 1 -m comment --comment "custom rule" -j LOG --log-prefix "custom rule "
        
```

Перезапустить межсетевой экран

Сбросить

Рисунок 160. Пользовательские правила

6.6 Удаленный доступ

WAF Dallas Lock позволяет создать удаленное подключение к автоматизированным рабочим местам в локальной вычислительной сети (LAN) из глобальной сети Интернет (WAN).

6.6.1 Основные настройки

На вкладке *Основные настройки* можно (см. Рисунок 161):

- включить/отключить возможность использовать **WAF Dallas Lock** для маршрутизации трафика из глобальной сети Интернет в локальную вычислительную сеть;
- настроить маршруты для клиентов, можно указать IP-адрес или IP-адрес подсети;



В маршрутах для клиентов указываются подсети или IP-адреса, к которым должны иметь доступ удаленные компьютеры.

- добавить файл корневого сертификата и файл списка отзывов сертификата.



По умолчанию используется корневой сертификат **WAF Dallas Lock** (см. 5.7.1 Серверные сертификаты).

[Основные настройки](#)
[Реквизиты для входа](#)

Удаленный доступ

Включить ☒

Маршруты для клиента

192.168.1.0/24 ✓ - +

192.168.250.0/24 ✓ - +

Корпоративные клиентские сертификаты

Файл корневого сертификата

Макс. размер: 1.00 MB

Файл списка отзыва сертификатов

Макс. размер: 1.00 MB

Сохранить

Применить

Сбросить

Рисунок 161. Основные настройки удаленного доступа

136

6.6.2 Реквизиты для входа

На данной странице возможно управление реквизитами для удаленного подключения. Для удаления реквизитов пользователя необходимо нажать кнопку **Удалить** (см. Рисунок 162). При активации чекбокса *Отключить* для пользователя доступ к локальной сети будет запрещен.

Основные настройки Реквизиты для входа ⓘ

Список реквизитов ⓘ

Имя	Описание	Отключить	Действия
test ✓	12	☐	Сгенерировать пароль Удалить

[Добавить](#)

[Сохранить](#) [Применить](#) [Сбросить](#)

Рисунок 162. Реквизиты для удаленного доступа

Для создания пользователя необходимо нажать кнопку **Добавить** и в открывшемся окне ввести имя пользователя, ключ безопасности и при необходимости добавить описание (см. Рисунок 163).

Добавление пользователя

Введите имя пользователя

Введите ключ безопасности

Добавьте описание

[Отменить](#) [Добавить](#)

Рисунок 163. Создание нового пользователя для удаленного доступа

Для изменения ключа безопасности пользователя необходимо нажать кнопку **Изменить ключ безопасности** и ввести новый ключ безопасности (см. Рисунок 164).

Изменение ключа безопасности:

Введите новый ключ безопасности

Повторите ключ безопасности

[Отменить](#) [Сохранить](#)

Рисунок 164. Изменение ключа безопасности пользователя

6.6.3 Создание удаленного подключения

Удаленный доступ предоставляется для клиентов под управлением операционных систем с использованием штатных средств для настройки протокола IKEv2:

- Windows 10 (22H2 и выше);
- Windows 11 (любая);
- операционных системы на базе Linux;
- Android.



Удаленное подключение доступно только из зоны WAN в зону LAN.

Для создания удаленного подключения на APM, с которого необходимо получить доступ к локальной сети, защищенной **WAF Dallas Lock**, необходимо установить сертификат CA Root WAF DL (см. 5.7.2 Сертификаты УЦ) в список доверенных корневых центров сертификации для компьютера.

Далее рассматривается процесс настройки удаленного подключения для операционной системы Windows 10. Для настройки на других операционных системах следует обратиться к документации, предоставленной их производителями.

В Windows 10 необходимо:

- скопировать загруженный сертификат на APM;
- открыть сертификат и нажать кнопку **Установить сертификат** (см. Рисунок 165);

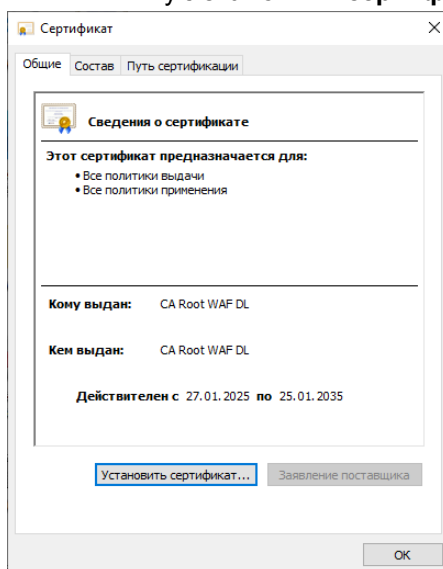


Рисунок 165. Установка корневого сертификата

- в открывшемся окне **Мастер импорта сертификатов** выбрать расположение хранилища: *Локальный компьютер* и нажать кнопку **Далее** (см. Рисунок 166);

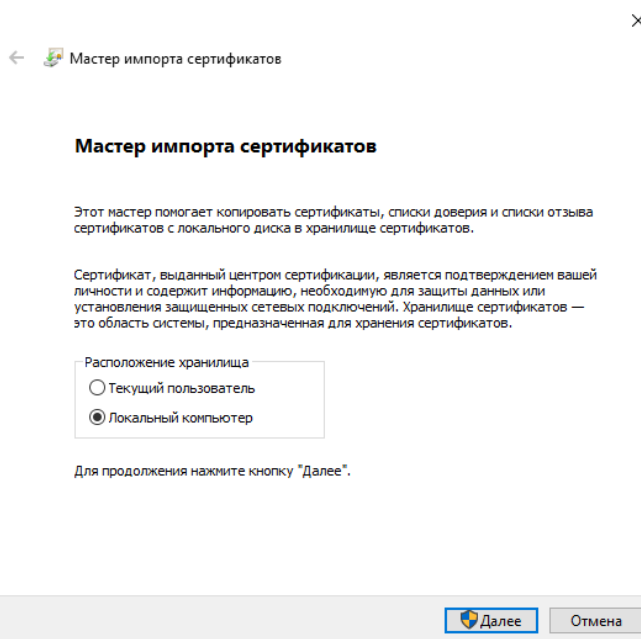


Рисунок 166. Выбор хранилища для корневого сертификата

- в открывшемся окне выбрать *Поместить все сертификаты в следующее хранилище* и нажать кнопку **Обзор**. Выбрать расположение *Доверенные корневые центры сертификации* и нажать кнопку **ОК** (см. Рисунок 167);

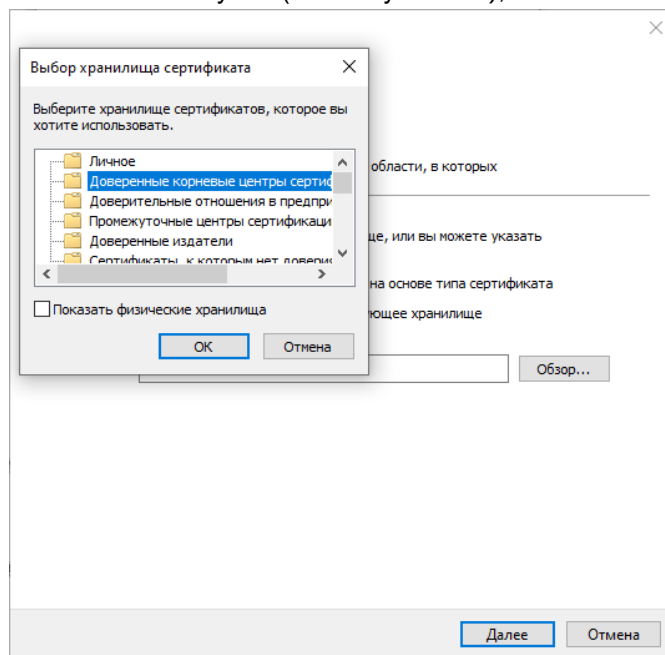


Рисунок 167. Выбор хранилища корневого сертификата

- нажать кнопку **Готово** (см. Рисунок 168);

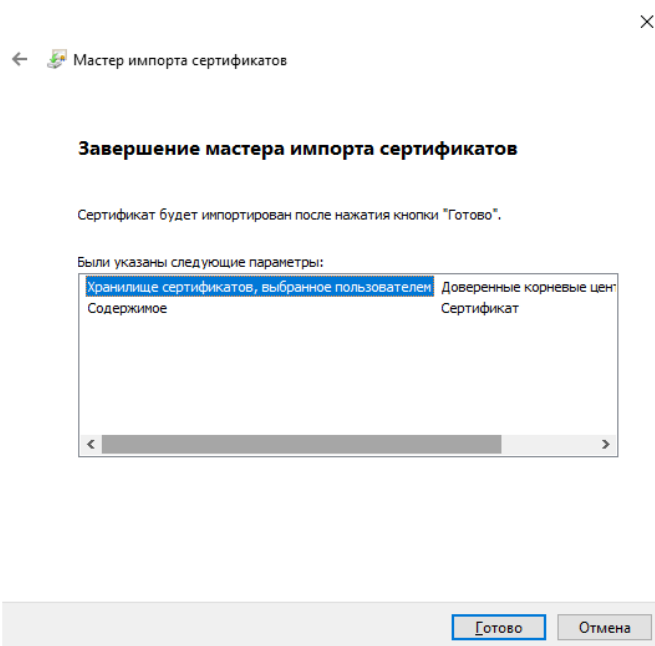


Рисунок 168. Завершение работы мастера импорта сертификатов

- в открывшемся окне нажать кнопку **ОК** (см. Рисунок 169).

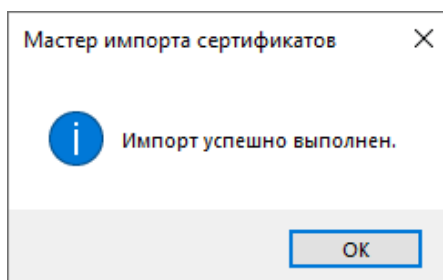


Рисунок 169. Импорт успешно выполнен

Возможны следующие варианты авторизации пользователей:

- по логину и паролю (см. 6.6.2 Реквизиты для входа);
- по сертификату (см. 5.7.3 Клиентские сертификаты).

Для настройки удаленного подключения необходимо:

- нажать кнопку **Пуск** и выбрать **Параметры** (значок шестеренки);
- в открывшемся окне выбрать **Сеть и Интернет**;
- в меню слева выбрать **VPN**;
- нажать кнопку **Добавить VPN-подключение**;
- настроить VPN подключение (см. Рисунок 170):
 - выбрать *Windows (встроенный)* в качестве поставщика VPN;
 - ввести имя подключения в поле *Имя подключения*;
 - ввести адрес сервера (адрес WAN-интерфейса **WAF Dallas Lock**) в поле *Имя или адрес сервера*;
 - выбрать *Протокол IKEv2* в поле *Тип VPN*;
 - выбрать тип данных для входа (*Имя пользователя и пароль* или *Сертификат*);
 - ввести имя пользователя и пароль, если в качестве типа данных для входа используются имя пользователя и пароль;
 - нажать **Сохранить**.
- если выбрана аутентификация по сертификату, то:
 - в панели управления перейти в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выбрать пункт **Настройки параметров адаптера**;
 - выбрать созданное VPN-подключение перейти его в свойства;
 - в открывшемся окне перейти во вкладку *Безопасность*;
 - выбрать пункт *Использовать сертификаты компьютеров* и нажать кнопку **ОК**.

При создании удаленного подключения с использованием клиентских сертификатов (см. 5.7.3 Клиентские сертификаты) требуется установить данный сертификат, для этого необходимо:



- скопировать загруженный сертификат на APM;
- открыть сертификат и нажать кнопку **Установить сертификат**;
- в окне **Мастер импорта сертификатов** выбрать расположение хранилища: *Текущий пользователь* и нажать кнопку **Далее**;
- в открывшемся окне выбрать *Поместить все сертификаты в следующее хранилище* и нажать кнопку **Обзор**.
- Выбрать расположение *Личное* и нажать кнопку **ОК**;
- нажать кнопку **Готово**.

- выбрать созданное подключение и нажать **Сохранить**.

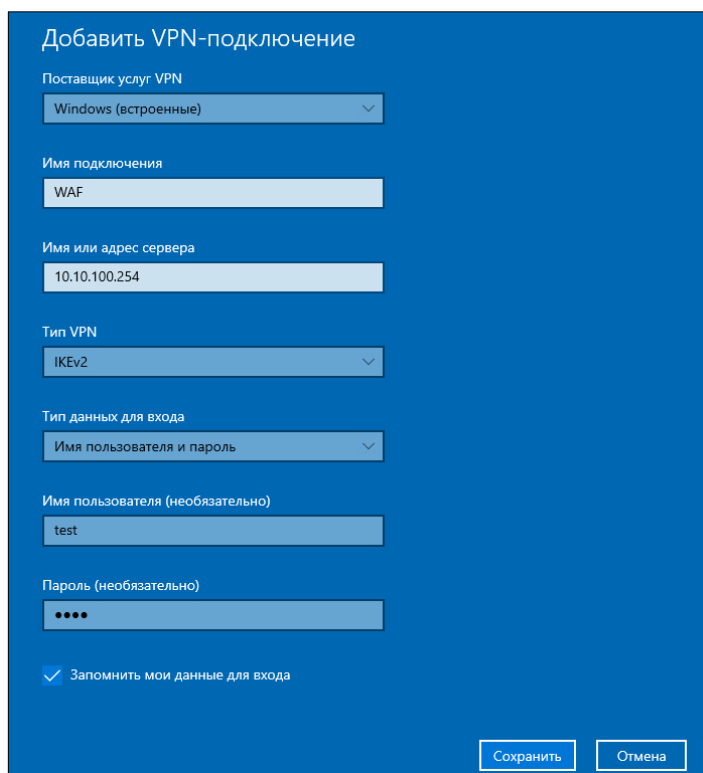


Рисунок 170. Настройка подключения по логину и паролю

6.7 Качество обслуживания (QoS)

На данной странице (см. Рисунок 171) 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.

Параметр *Ограничить журнал сообщений* позволяет настроить количество журналируемых QoS событий за определенный период.



При заполнении поля *Ограничить журнал сообщений* используются суффиксы «s (second)» — для указания секунд, «m (minute)» — минут, «h (hour)» — часов, «d (day)» — дней.

Параметр не может быть установлен на значение свыше 120 журналируемых событий в секунду.

Интерфейсы. В данном разделе можно задать индивидуальные настройки качества обслуживания для интерфейсов (wan, wan6, lan, dmz). Для этого необходимо в раскрывающемся меню выбрать интерфейс и нажать кнопку **Добавить**. Управление параметрами QoS для интерфейса включает в себя изменение следующих параметров:

- *Включить.* Чекбокс управляет работой QoS для выбранного интерфейса.
- *Подсчитывать возможное превышение трафика.* Чекбокс управляет функцией определения возможного превышения трафика для выбранного интерфейса.
- *Скорость передачи данных.* Настройка максимальной ширины канала для выбранного интерфейса.

Правила классификации. В данном разделе можно настроить приоритет по IP-адресам и для назначения результирующего решения о пропуске трафика, указав в настройках хост источника и хост назначения, протокол, порты, максимальную пропускную способность, комментарий и параметры журналирования для выбранного правила. Параметр *Назначение* может принимать следующие значения:

- *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 привилегированными назначениями, этому классу будет выделен только 1% от общего установленного лимита. Это назначение используется 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.

Ограничить журнал сообщений
10/minute

Интерфейсы

WAN

Включить
Подсчитывать возможное превышение трафика
Скорость передачи данных (кбит/с)
128

-- Выберите интерфейс --
Добавить

Правила классификации

Назначение	Хост источника	Хост назначения	Протокол	Порты	Количество байт	Комментарий	Настройка журнала	Сортировка	
приоритетный	всего	всего	всего	22.53		ssh, dns			Удалить
обычный	всего	всего	TCP	20.21.25.80, 110.443		ftp, smtp, http(s), imap			Удалить
экспресс	всего	всего	всего	5190		ADL, iChat, ICQ			Удалить

Добавить +

Сохранить
Применить
Сбросить

Рисунок 171. Качество обслуживания (QoS)

6.8 Диагностика

На данной странице (см. Рисунок 172) можно произвести диагностику работы системы — проверить доступность ресурса ping-запросом по IP-адресу или сетевому имени, выполнить трассировку маршрута и таким образом проверить доступность сервера, а также выполнить DNS-запрос.

Результаты выполнения той или иной команды предоставляются ниже на странице.

Информационная панель
Журналы и статистика
Настройки
Сеть
Диагностика
Перезагрузка
Выйти

www.dallaslock.ru
Пинг-запрос
www.dallaslock.ru
Трассировка
www.dallaslock.ru
DNS-запрос

Рисунок 172. Диагностика