УТВЕРЖДЕН
ПФНА.501540.001 34-ЛУ

ШЛЮЗ БЕЗОПАСНОСТИ

WAF Dallas Lock

(версия изделия 2.12.10.2)

Руководство оператора (пользователя)

ПФНА.501540.001 34

Листов 10

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Данное руководство предназначено для пользователей рабочих станций, которые входят в защищенную шлюзом безопасности **Web Application Firewall (WAF) Dallas Lock** сеть.

В руководстве содержатся сведения, необходимые пользователю для работы в защищенной **WAF Dallas Lock** сети.

В документе представлены элементы графических интерфейсов, которые соответствуют эксплуатации **WAF Dallas Lock**. Следует обратить внимание, что элементы графического интерфейса могут иметь незначительные отличия от представленных.

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, возможность 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, обнаружения и предотвращения вторжений;
- анализ поведения пользователей, обнаружение аномальной активности и блокировка трафика на основании графов связей и переходов на защищаемом ресурсе;
- интеграция с **Единым центром управления Dallas Lock**;
- интеграция в SIEM-систему по протоколу syslog в формате leef;
- 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) (Рисунок 1).

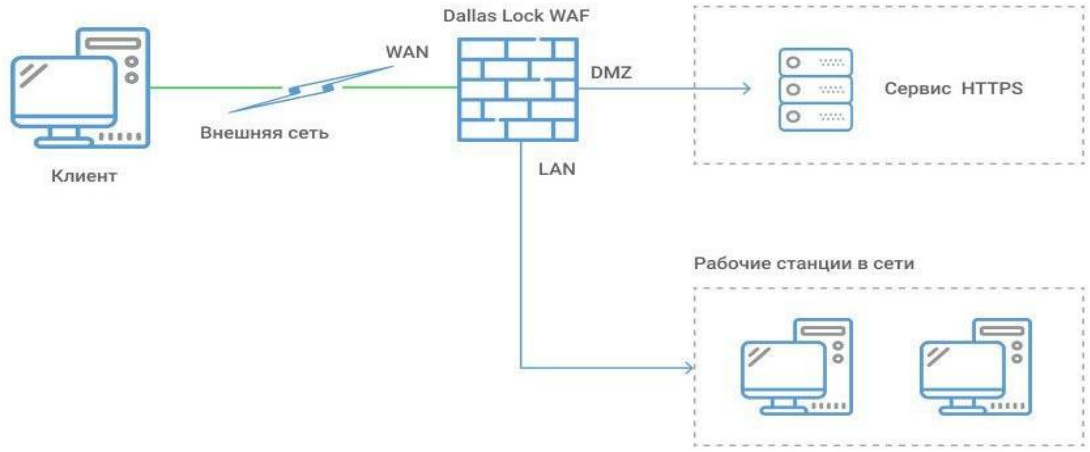

Рисунок 1. Типовая схема использования «WAF Dallas Lock»

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

фильтрации и баз сигнатур атак.

Существует два режима работы **WAF Dallas Lock**: штатный и аварийный.

В штатном режиме работы **WAF Dallas Lock** выполняет функции, описанные в пункте 1.1 Назначение и возможности.

В аварийном режиме работы происходит блокировка всего проходящего информационного потока (трафика), кроме информационного потока для управления **WAF Dallas Lock** и передачи данных на ЕЦУ, причем управление может осуществляться только из LAN уполномоченным пользователем. Для этого происходит остановка всех сервисов, кроме сервисов из заранее определенного «белого» списка.

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 посредствам 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**.

К основным принципам безопасности работы **WAF Dallas Lock** относятся:

1) Выполнение ограничений по эксплуатации **WAF Dallas Lock**, перечисленных в п.3.3 документа ПФНА.501540.001 ФО Формуляр.
2) Осуществление работы **WAF Dallas Lock** строго в соответствии с эксплуатационной документацией.

1.3 Структура и составные модули

Меню управления **WAF Dallas Lock** расположено в верхней части страницы и представлено на рисунке 2.

1. Основное меню с набором вкладок.
2. Имя пользователя и хоста.
3. Иконки, содержащие следующую информацию:
   - права администрирования изделия;
   - общее количество сохраненных, но не принятых конфигурационных изменений изделия (иконка не отображается, если все изменения были приняты);
   - вкл./выкл. автоматическое обновление изделия;
   - иконка регистрации изделия в домене безопасности **ЕЦУ** (иконка не отображается, если изделие не зарегистрировано в домене безопасности);
   - переключение между светлой и темной темой графического интерфейса изделия.

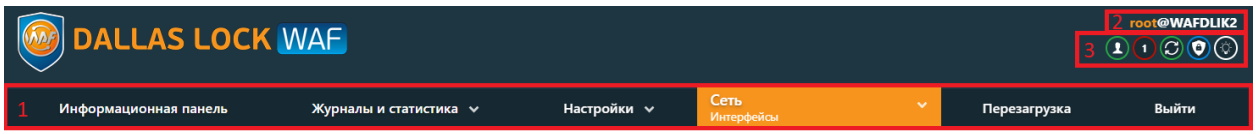

Рисунок 2. Меню управления WAF Dallas Lock

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

1. **Информационная панель.** Набор виджетов и блоков статистических данных.
2. **Журналы и статистика**. Подсистема учета и регистрации событий в **WAF Dallas Lock**.
3. **Настройки.** Подсистема тонкой настройки **WAF Dallas Lock**.
4. **Сеть.**
5. **Перезагрузка.** При нажатии произойдет перезагрузка изделия.
6. **Выйти.** Выйти из меню на страницу авторизации сменить пользователя.

2 БЕЗОПАСНОСТЬ СРЕДСТВА ПРИ РАБОТЕ ПОЛЬЗОВАТЕЛЯ (АУДИТОРА)

2.1 Параметры (настройки) безопасности средства, доступные пользователю

Доступ к управлению и права для работы пользователя в **WAF Dallas Lock** назначаются администратором **WAF Dallas Lock** из строго предопределенного списка. Для пользователя может быть настроена роль безопасности аудита с помощью следующих параметров (Рисунок 3):

- разрешить или запретить квитирование (подтверждение инцидентов ИБ);
- задать права на просмотр всех или определенных журналов;
- задать права на просмотр всех или определенных вкладок блока **Настройки** изделия;
- задать права на просмотр всех или определенных вкладок блока **Сеть** изделия.

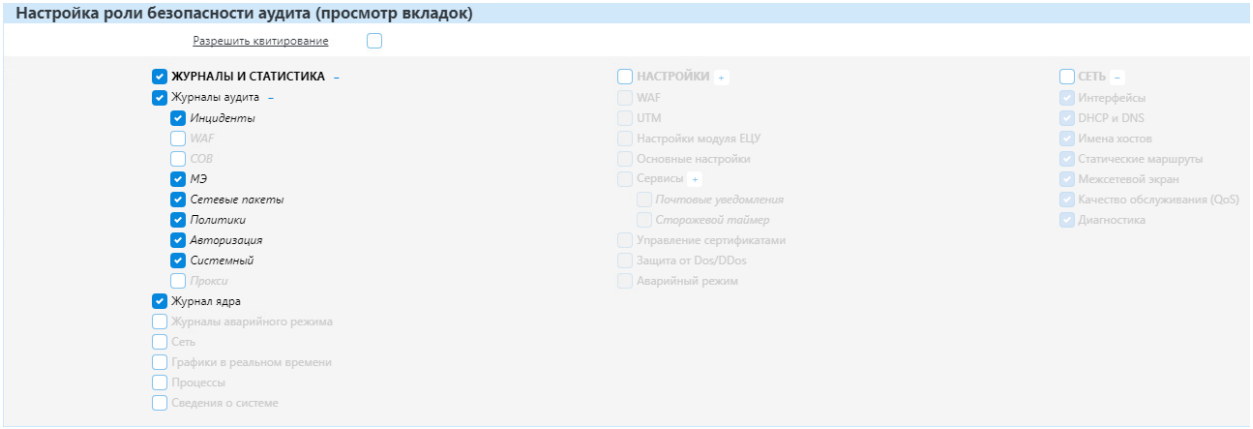

Рисунок 3. Настройка роли безопасности аудита

Параметры безопасности изделия, доступные пользователю:

- вход в систему и смена пароля в соответствии с правилами (если разрешено администратором **WAF Dallas Lock**);
- мониторинг и анализ событий безопасности;
- возможность подтверждать атаки и инциденты ИБ;
- просмотр графа связей и переходов на защищаемом ресурсе;
- взаимодействие с администратором **WAF Dallas Lock** в случае нештатных ситуаций.

Типы событий безопасности, связанные с доступными пользователю функциями **WAF Dallas Lock**:

- вход в систему (события аутентификации);
- проведение аудита;
- информирование об атаке;
- информирование о переходе **WAF Dallas Lock** в аварийный режим.

Подробное описание графа связи и переходов на защищаемом ресурсе, мониторинга и анализа событий безопасности содержится в документе «Руководство по эксплуатации» ПФНА.501540.001.

Для выполнения входа в консоль управления **WAF Dallas Lock** необходимо пройти процедуру аутентификации с учетными данными пользователя (Рисунок 4).

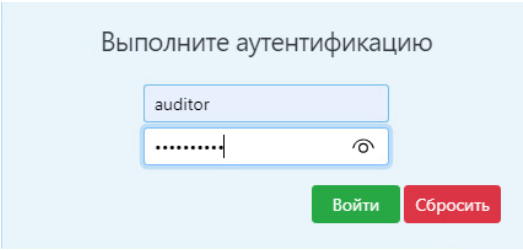

Рисунок 4. Ввод учетных данных

Учетная запись пользователя, зарегистрированного в **WAF Dallas Lock**, имеет следующие атрибуты, которые необходимы непосредственно для входа.

Основные	
Имя (логин)	За пользователем закрепляется условное имя (идентификатор), необходимое для идентификации его в **WAF Dallas Lock**
Пароль	Пользователю сообщается пароль, который необходим для подтверждения того, что именно он является пользователем, зарегистрированным под этим именем (происходит аутентификация)

Пользователю необходимо:
- уточнить у администратора все авторизационные данные для входа;
- запомнить свое имя и пароль;
- никому не сообщать пароль и данные учетной записи.

Возможна ситуация, при которой пользователь забыл свой пароль. В этом случае он также должен обратиться к администратору, который имеет право назначить пользователю новый пароль.

Авторизация пользователя осуществляется при каждом входе. При этом в **WAF Dallas Lock** установлены следующие правила:

Для имени:
- минимальная длина имени — 1 символ;
- имя может содержать латинские символы и цифры;
- разрешается использовать различные регистры клавиатуры и цифры, при этом нужно помнить, что прописные и строчные буквы воспринимаются как различные (User и user являются разными именами).

Для пароля:
- минимальная длина пароля — 8 символов;
- пароль должен содержать цифры, специальные символы, различные регистры клавиатуры, при этом нужно помнить, что прописные и строчные буквы воспринимаются как различные (Password и password являются разными паролями).

Для входа на **WAF Dallas Lock** каждому пользователю предлагается выполнить следующую последовательность шагов.

1. Заполнить поле имени пользователя, под которым он зарегистрирован в **WAF Dallas Lock**.

При вводе имени и пароля переключение раскладки клавиатуры (русская/латинская) производится нажатием комбинации клавиш, установленной при настройке свойств клавиатуры. Текущий язык отображается индикатором клавиатуры.

2. Ввести пароль. При вводе пароля поле для ввода является текстовым. Однако на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «●» (точка).

Администратором **WAF Dallas Lock** может быть назначена аутентификация без пароля. В таком случае вход осуществляется по логину, ввод каких-либо символов в поле пароля повлечет за собой ошибку входа (Рисунок 5).

3. При вводе пароля следует помнить, что строчные и прописные буквы различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля.
4. Нажать кнопку **Enter** на клавиатуре или кнопку **Войти** на панели авторизации.

После нажатия кнопки **Enter** на клавиатуре или кнопки **Войти** на панели авторизации в системе защиты сначала проверяется возможность входа пользователя с данным именем и правильность указанного пользователем пароля. В случае успеха проверки пользователю разрешается вход в систему, иначе вход в систему пользователю запрещается. При этом на экран могут выводиться сообщения о причине запрета или соответствующие сообщения предупреждающего характера.

Если введенный пароль неверен, то на экране появится сообщение об ошибке, после чего система защиты предоставит возможность повторно ввести имя и пароль (Рисунок 5).

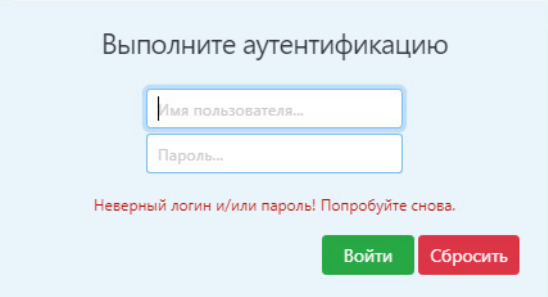

Рисунок 5. Сообщение при вводе неправильного пароля

Администратор **WAF Dallas Lock** может настроить количество попыток входа и время блокировки учетной записи пользователя при превышении этого показателя. Следует уточнить у администратора эти параметры.

Администратором может быть назначена принудительная смена пароля при первом входе в систему, в таком случае необходимо указать новый пароль в открывшейся вкладке.

Для смены пароля необходимо перейти на вкладку **Настройки**, выбрать раздел **Пароль пользователя** (Рисунок 6).

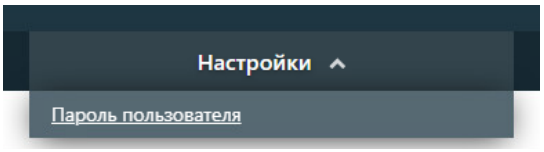

Рисунок 6. Раздел «Пароль пользователя»

Пользователю может быть не предоставлено разрешение о последующей смене пароля. Для смены пароля стоит обращаться к администратору **WAF Dallas Lock**.

В открывшемся диалоговом окне необходимо ввести в соответствующие поля старый пароль, новый пароль и подтверждение нового пароля. Пользователь также может ввести сгенерированный программой пароль, нажав . Далее нужно нажать кнопку **Применить** для сохранения нового пароля (Рисунок 7).

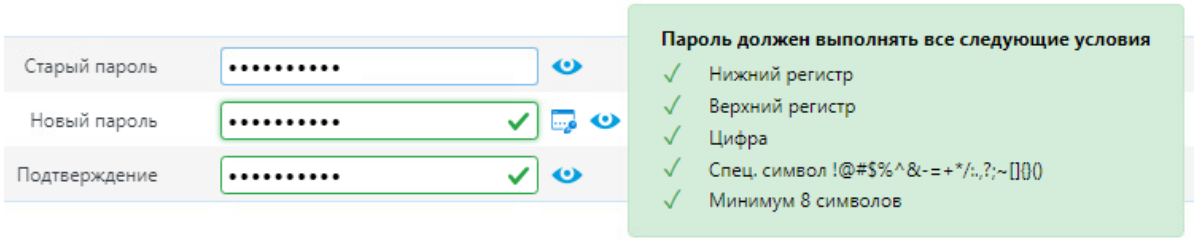

Рисунок 7. Смена пароля

Сложные пароли при их регулярной смене снижают вероятность успешной атаки на пароль. Пароль должен соответствовать требованиям безопасности и содержать:

- нижний регистр;
- верхний регистр;
- цифру;
- специальный символ;
- минимум 8 символов.

Если все требования соблюдены, то пароль пользователя будет успешно сменен, появится соответствующее сообщение (Рисунок 8). Далее вход пользователя в оболочку **WAF Dallas Lock** будет осуществляться с новым паролем.

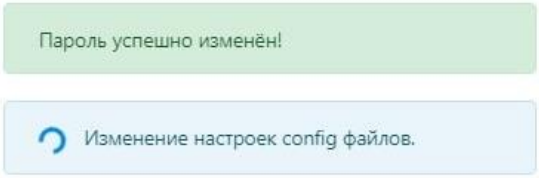

Рисунок 8. Успешная смена пароля

2.2 Сбои и ошибки эксплуатации средства

Таблица 1 — Всплывающие ошибки при эксплуатации средства

Текст ошибки	Описание	Решение
Неверный логин и/или пароль! Попробуйте снова	Введены неверные данные для входа в систему. Событие возникает в связи с отсутствием учетной записи или предоставлением неверного пароля к ней	Необходимо обратиться к администратору **WAF Dallas Lock**
К сожалению, вы ввели неверный логин и/или пароль слишком много раз. Пожалуйста, возвращайтесь позже	Пароль введен неверно несколько раз (допустимое количество попыток ввода пароля указывается в настройках системы)	
Недостаточно прав	Событие возникает при попытке запустить команду, для которой необходимы права администрирования	
Ошибка получения данных	Ошибка возникает при попытке получить системный журнал	
Введенные пароли не совпадают, пароль не изменен!	Введенный пароль не совпадает с паролем в подтверждении	Необходимо заново ввести пароль в двух полях
Пароль совпадает со старым, пароль не изменен!	Новый пароль совпадает со старым паролем.	Необходимо ввести новый пароль отличающийся от старого как минимум на один символ
Can't load access ipv4 rules	Не получается получить доступ к правилам IPv4	Необходимо обратиться к администратору **WAF Dallas Lock**

Во всех сложных ситуациях при работе с **WAF Dallas Lock**, которые пользователь не в состоянии разрешить самостоятельно, необходимо обращаться к администратору **WAF Dallas Lock**.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Некоторые термины, содержащиеся в тексте руководства, уникальны для **WAF Dallas Lock**, другие используются для удобства, третьи выбраны из соображений краткости.

WAF	Web Application Firewall
SIEM	Security information and event management
DMZ	(Demilitarized Zone) демилитаризованная зона
LAN	(Local area network) локальная вычислительная сеть
WAN	(Wide Area Network) глобальная компьютерная сеть
ЕЦУ	Единый центр управления «Dallas Lock»
ИБ	Информационная безопасность