



Ш Л Ю З Б Е З О П А С Н О С Т И

WAF DALLAS LOCK

**МЕЖСЕТЕВОЙ ЭКРАН ПРИКЛАДНОГО УРОВНЯ
WAF DALLAS LOCK**

ОБЗОР



КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ



СОДЕРЖАНИЕ

Введение 1

1. Ключевые преимущества WAF Dallas Lock 1

2. Функциональные возможности 3

3. Основные сценарии применения 4

4. Интеграция с ЕЦУ Dallas Lock 5

5. Сертификация и область применения 6

Заключение 7



Размещаемая в данном документе информация предназначена для свободного ознакомления. Центр защиты информации ООО «Конфидент» оставляет за собой право вносить без уведомления любые изменения в данный документ, а также в ПО, которое описано в документе.

ВВЕДЕНИЕ WAF Dallas Lock — сертифицированный межсетевой экран прикладного уровня, предназначенный для защиты веб-серверов, обслуживающих сайты, веб-службы и веб-приложения, от сетевых атак и нежелательного интернет-трафика.

Изделие включает два функциональных модуля:



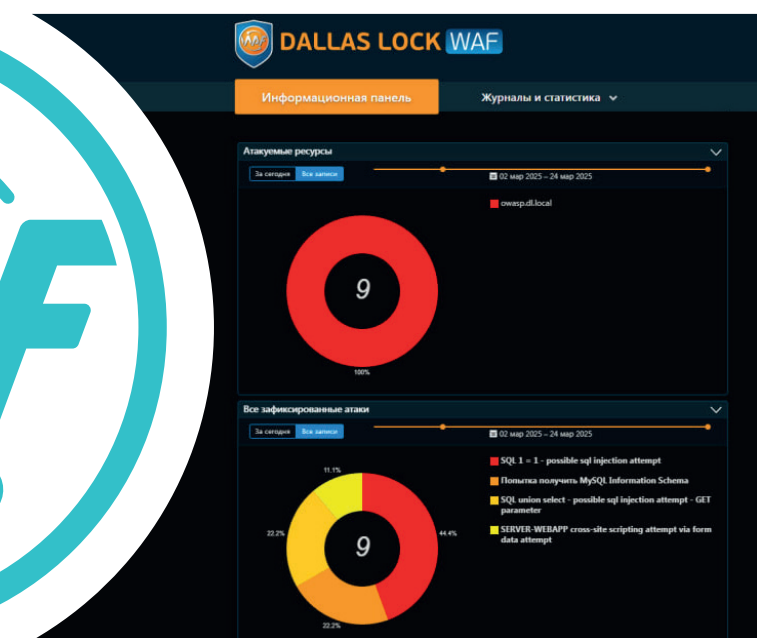
WAF (Web Application Firewall)
межсетевой экран уровня веб-приложений.



UTM (Unified Threat Management)
межсетевой экран уровня логических границ сети и система обнаружения вторжений уровня сети.

1. КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА WAF DALLAS LOCK

- **Многоуровневая защита «из коробки».**
Закрывает сразу три уровня: прикладной, сетевой и транспортный. Не нужно покупать отдельные средства для каждого уровня.
- **Интеллектуальный анализ трафика.**
Сигнатурный и эвристический методы усилены нейронной сетью, что позволяет выявлять даже неизвестные ранее атаки.
- **Быстрое внедрение.**
Установка «в два клика» с мастером первичных настроек и автоматическим подбором правил защиты под ваш ресурс.
- **Отказоустойчивость.**
Работа в кластере active-passive гарантирует непрерывную защиту даже при сбоях оборудования.
- **Гибкое развёртывание.**
Поставка в виде ISO-образа для установки на физическую платформу или виртуальные машины (VMware ESXi, VMware Workstation, Hyper-V, VirtualBox).
- **Единая экосистема Dallas Lock.**
Полная интеграция с ЕЦУ Dallas Lock для централизованного управления всей инфраструктурой безопасности.



**МЕЖСЕТЕВОЙ ЭКРАН
ПРИКЛАДНОГО УРОВНЯ**

2. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ (WAF):

- защита от угроз из списка OWASP TOP 10: XSS, CSRF, brute-force-атаки, SQL-инъекции;
- анализ трафика веб-приложений: XML-API и JSON-API, поддержка HTTP/2/3, инспекция SSL/TLS;
- GEO-IP-фильтрация для разграничения доступа по географии;
- анализ поведения пользователей с помощью графа связей и переходов на защищаемом ресурсе;
- использование нейронной сети для анализа входящего трафика.

ЗАЩИТА СЕТЕВОЙ ИНФРАСТРУКТУРЫ (UTM):

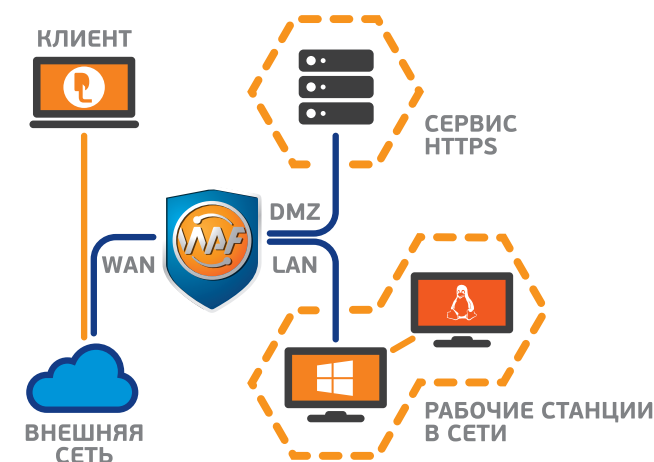
- защита от DoS/DDoS атак на 7 и 4 уровнях модели OSI;
- контроль и фильтрация сетевых пакетов в соответствии с заданными правилами;
- регулярно обновляемая база решающих правил;
- интеграция с SIEM-системами по протоколу syslog в формате LEEF;
- удалённое подключение к APM — возможность создания защищённого соединения из зоны WAN в зону LAN через WAF Dallas Lock.

УПРАВЛЕНИЕ И МОНИТОРИНГ:

- графическая панель мониторинга с диаграммами и статистикой в реальном времени;
- гибкая настройка правил и политик фильтрации трафика;
- автоматическое типизирование защищаемого ресурса — по результатам сканирования определяется сервер, фреймворк и CMS, после чего подбираются оптимальные пресеты правил;
- гибкая ролевая модель с предустановленными ролями, шаблонами доступа и возможностью создания пользовательских карт доступа к меню WAF Dallas Lock;
- централизованный мониторинг и управление защитой нескольких веб-приложений из единой консоли;
- мастер первичных настроек при первом входе - пароль администратора, лицензия, SSH, DNS;
- журналы и статистика удалённых соединений с возможностью их принудительного разрыва;
- просмотр содержимого атакующих и вредоносных пакетов - детальная информация о сработавшем правиле: ID, пресет, тип события, уровень атаки, источник, направление и другие параметры для глубокого анализа инцидентов.

3. ОСНОВНЫЕ СЦЕНАРИИ ПРИМЕНЕНИЯ

WAF Dallas Lock предназначен для защиты веб-серверов в демилитаризованной зоне (DMZ) и сетевой инфраструктуры (LAN) от угроз, исходящих из глобальной сети (WAN). Для удобства фильтрации реализовано разделение физических интерфейсов на зоны — за каждой закреплён собственный профиль межсетевого экрана.



Схемы работы.

- Обратный прокси-сервер — принимает и анализирует трафик перед передачей на защищаемый ресурс.
- Прозрачный прокси-сервер — проверяет трафик без изменения маршрута.
- Мониторинг — фиксирует события безопасности без вмешательства в трафик.

Основные сценарии использования:

- оперативное выявление и реагирование на атаки;
- ведение централизованного аудита событий ИБ и состояния системы защиты;
- отслеживание инцидентов в динамике через диаграммы и графики;
- защита и мониторинг веб-приложений в режиме 24/7.

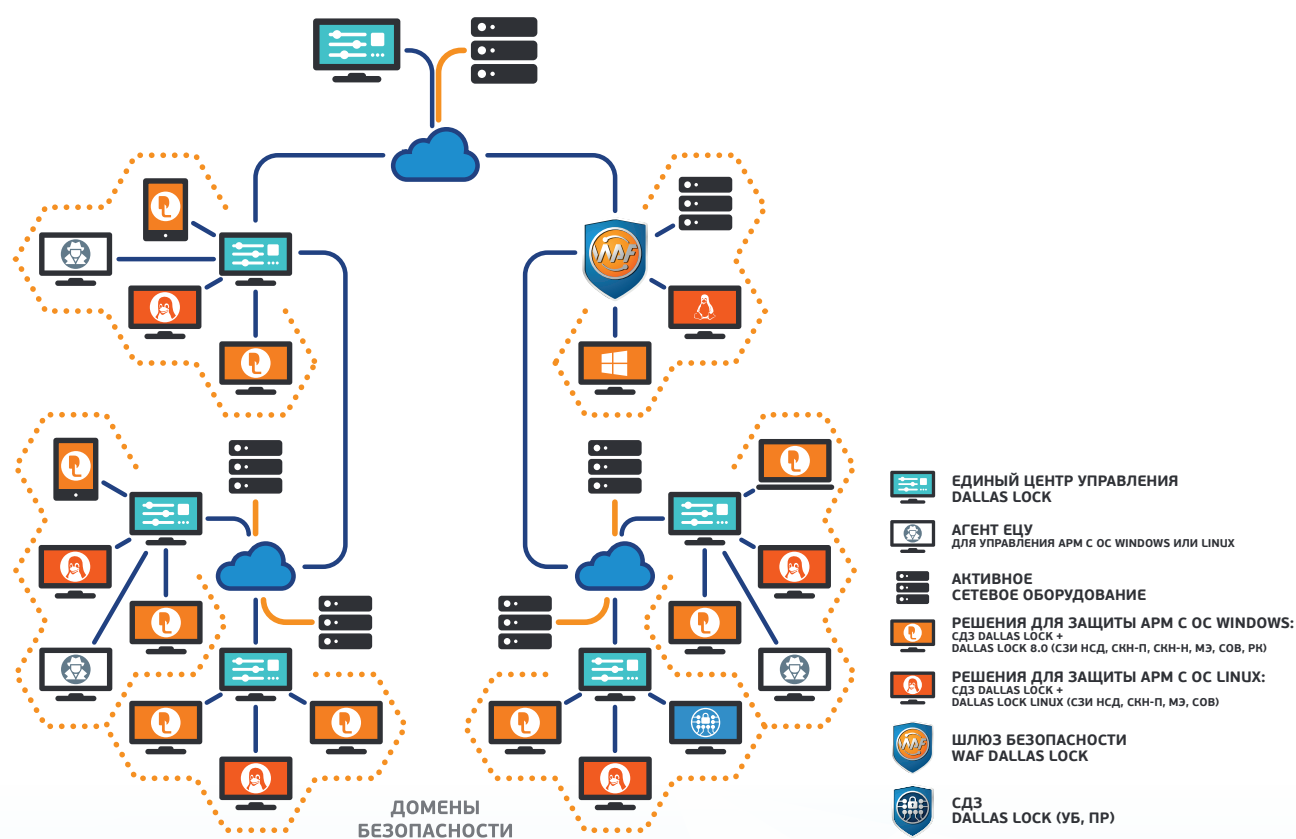


Ш Л Ю З Б Е З О П А С Н О С Т И

WAF DALLAS LOCK

4. ИНТЕГРАЦИЯ С ЕЦУ DALLAS LOCK

Единый центр управления Dallas Lock — кроссплатформенное средство централизованного управления, контролирующее безопасность всей ИТ-инфраструктуры организации вне зависимости от её структуры и масштабов. ЕЦУ предназначен для контроля целостности настроек активного сетевого оборудования и управления всеми решениями продуктовой линейки Dallas Lock, включая WAF Dallas Lock.



Ключевые возможности взаимодействия ЕЦУ с WAF Dallas Lock:

- регистрация в ЕЦУ для централизованного мониторинга;
- оповещение об инцидентах безопасности;
- активация и деактивация аварийного режима;
- выключение и перезагрузка WAF Dallas Lock;
- сброс до заводских настроек и сброс временных блокировок;
- сбор и просмотр журналов аудита;
- сохранение и применение файла конфигураций;
- обновление базы решающих правил (БРП) и контроль целостности изделия.

5. СЕРТИФИКАЦИЯ И ОБЛАСТЬ ПРИМЕНЕНИЯ



Изделие соответствует требованиям ФСТЭК России (сертификат № 4863 от 08.10.2024):

- 4 класс защиты МЭ по «Профилю защиты межсетевых экранов типа «Г» (ИТ.МЭ.Г4.ПЗ).
- 4 класс защиты МЭ по «Профилю защиты межсетевых экранов типа «Б» (ИТ.МЭ.Б4.ПЗ).
- 4 класс защиты СОВ уровня сети по «Профилю защиты систем обнаружения вторжений уровня сети четвертого класса» (ИТ.СОВ.С4.ПЗ).
- 4 уровень доверия по «Требованиям по безопасности информации».



Включён в единый реестр российских программ для ЭВМ и БД (реестровая запись № 21831 от 15.03.2024 г.).

Продукт может применяться:

- для защиты значимых объектов КИИ до 1 категории значимости включительно;
- в ГИС до 1 класса защищённости включительно;
- в ИСПДн до 1 уровня защищённости включительно;
- в АСУ ТП до 1 класса защищённости включительно;
- в АС до класса защищённости 1Г включительно.

Системные требования:

- процессор (x86-64): 2 ГГц, 4 ядра;
- оперативная память: 8 Гб;
- накопитель: не менее 32 Гб + 128 Гб для журналов аудита;
- наличие режима совместимости (MBR) в BIOS;
- сетевые интерфейсы: не менее 3 (RJ45 / SFP+) для зон LAN, WAN, DMZ.

ЗАКЛЮЧЕНИЕ WAF Dallas Lock — это комплексное сертифицированное решение для защиты веб-приложений и сетевой инфраструктуры, позволяющее обеспечить надёжную защиту в АС, ИСПДн, ГИС, АСУ ТП и на объектах КИИ.

Благодаря сочетанию модулей WAF и UTM, использованию нейронных сетей, гибкой ролевой модели, быстрой установке и интеграции с ЕЦУ Dallas Lock продукт обеспечивает эффективную защиту при минимальных затратах на внедрение и администрирование.





192029, г. Санкт-Петербург
пр. Обуховской Обороны, д. 51, лит. К
телефон/факс: (812) **325-1037**

<http://www.confident.ru/>
<http://www.dallaslock.ru/>
e-mail:

isc@confident.ru - коммерческие вопросы
helpdesk@confident.ru - техническая поддержка

Схема проезда:



www.confident.ru



www.dallaslock.ru



Telegram-канал

