

Описание платформы

Сентябрь 2026
Версия 1.8.0

Все авторские права на эксплуатационную документацию защищены.

Документ входит в комплект поставки программного обеспечения. Без специального разрешения этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию или передаче третьим лицам, или иному использованию с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю.

Обзор платформы

Программный комплекс «Многоуровневая защита веб-приложений Frisbee WAF» представляет собой межсетевой экран прикладного уровня, предназначенный для защиты веб-приложений от интернет-угроз.

Платформа включает брандмауэр, систему обнаружения вторжений и фильтр запросов к веб-приложениям. Предназначена для защиты высоконагруженных приложений.

Развертывается на физическом сервере, виртуальной машине, клауд-платформе или в составе программно-аппаратного комплекса (ПАК).

Минимальные системные требования для работы Frisbee WAF

Минимальные системные требования для работы Frisbee WAF приведены в таблице 1.

Таблица 1 – Минимальные системные требования для работы Frisbee WAF

Компонент	Минимальные требования
Объем оперативной памяти	Не менее 16 ГБ
Процессор	8-ядерный и более с архитектурой x86-64, поддержкой инструкций SSE 4.2 и AVX, тактовая частота — не ниже 2,2 ГГц
Объем жесткого диска	Не менее 500 Гбайт
Сетевые интерфейсы	Не менее 2 × 1 Гбит Ethernet

В Frisbee WAF поддерживаются два режима кластеризации:

- Active-Standby — один узел активен, второй в режиме ожидания.
- Active-Active — оба узла обрабатывают нагрузку одновременно.

Для настройки кластера Frisbee WAF необходимо два сервера с системными требованиями, приведенными в таблице 2.

Таблица 2 – Минимальные системные требования для каждого сервера Frisbee WAF

Компонент	Минимальные требования
Объем оперативной памяти	Не менее 16 ГБ
Процессор	8-ядерный и более с архитектурой x86-64, поддержкой инструкций SSE 4.2 и AVX, тактовая частота — не ниже 2,2 ГГц
Объем жесткого диска	Не менее 500 Гбайт
Сетевые интерфейсы	3 × 1 Гбит Ethernet

Платформа работает на операционной системе Debian 12/Astra Linux Special Edition 1.8.

Возможности платформы

- Анализ трафика веб-приложений и обнаружение атак (вторжений);
- Блокирование попыток сетевых атак при работе с веб-приложениями;
- Защита веб-приложений от основных типов угроз;
- Обнаружение подозрительной активности;
- Настройка защитных механизмов Frisbee WAF под конкретное защищаемое приложение;
- Контроль доступа к функциям и регистрация действий пользователей защищаемых приложений;
- Интеграция с внешними системами управления событиями информационной безопасности и системами управления задачами;
- Настройка балансировщика;
- Возможность работы в режиме Active/Passive (отказоустойчивый кластер);
- Настройка multiple CORS для заведенных за Frisbee WAF серверов;
- Создание групп пользователей (организаций) и управление ими;
- Мультитенантность (работа нескольких изолированных друг от друга ресурсов в рамках одного сервиса с разделением глобальных и локальных групп пользователей, определение их полномочий);
- Использование технологии машинного обучения;

- Проверка CAPTCHA на уровне сервера или локации, в том числе после срабатывания ограничения числа запросов;
- Детектор аномалий (Anomaly Detector): модуль машинного обучения для анализа трафика защищаемых приложений, обучения модели нормального поведения и выявления аномальных запросов с учётом ложных срабатываний;
- Расширенное управление детектором инъекций и ML: глобальное включение и отключение, порог срабатывания, белый список ML;
- Разграничение доступа к журналам Access Logs и Audit по организации;
- Отправка событий аудита во внешнюю систему SIEM;
- Централизованное управление статическими маршрутами (хранилище в базе данных платформы);
- Открытый API, включая Events API v2 (взаимодействие через специальный токен доступа).

Специфика работы платформы

- В процессе работы Frisbee WAF опирается на модели нормального поведения защищаемого приложения, выявляя аномалии. Аномалии и другие атрибуты (пользователь, сессия, действие и др.) привязываются к HTTP-транзакциям (парам запрос–ответ);
- Группы транзакций объединяются в события, которые имеют время жизни и свидетельствуют о тех или иных аномалиях в работе Frisbee WAF или веб-приложения.

Поддерживаемые типы угроз

- Всевозможные виды инъекций (SQL injection, OS injection, RCE, XPath-injection, XXE);
- Реализация атак на обратный путь в директориях и на включение удаленных или локальных файлов (Directory traversal, Remote/Local File Inclusion);
- Межсайтовый скриптинг (XSS);
- Межсайтовая подделка запросов (CSRF);
- Реализация переборных атак (bruteforce);
- «Умный» DoS (application-level DoS);
- Автоматизированный обход приложения, массовое скачивание информации, использование сканеров уязвимостей (web scraping, automation).

Где может применяться

В компаниях, проектах с высоким уровнем требований к информационной безопасности, работающих в следующих сферах:

Финансовые технологии. Банковские и финансовые платформы. Использование в банковской и финансовой сферах на платформах (веб-сайтах, приложениях интернет-банкинга, внутренних информационных системах и других сервисах) оказания финансовых услуг, обеспечения взаимодействия потребителей финансовых услуг и финансовых организаций.

Розничная торговля. Платформы продажи товаров потребителям — частным лицам, приобретение либо продажа изделий для личного, семейного, домашнего и иного подобного использования.

Онлайн-торговля, электронная коммерция. Проекты в сфере e-commerce, которые включают электронную покупку или продажу товаров через онлайн-сервисы или через интернет, мобильную коммерцию, электронные переводы средств, управление цепочками поставок, интернет-маркетинг, онлайн-обработку транзакций, электронный обмен данными (EDI), системы управления запасами и автоматизированные системы сбора данных.

IT-компании, разрабатывающие микросервисы. Проекты по созданию единого приложения или платформы как набора отдельных сервисов, каждый из которых работает в собственном процессе и коммуницирует с остальными, используя легковесные механизмы. Данные сервисы объединяются под конкретные бизнес-потребности и развертываются независимо с использованием полностью автоматизированной среды.

Промышленность. Информационные системы и сервисы сбора, хранения и анализа данных, внутренние корпоративные информационные системы, программное обеспечение для интеллектуальной и эффективной добычи природных ресурсов, переработки сырья, производства машин, механизмов и других средств, предметов и устройств.

Государственные информационные системы. Проекты, созданные для реализации полномочий государственных органов, обмена информацией между ними, обеспечения эффективного оказания административных процедур, а также в иных целях. В данных системах аккумулируется огромное количество статистических данных, собираемых в соответствии с компетенцией государственных органов.

Онлайн-лотереи и казино. Платформы или программы, разработанные в целях предоставления пользователям доступа к участию в лотереях и азартных играх в онлайн-формате.

Преимущества платформы

Легкий старт

Время от начала установки до ввода в эксплуатацию платформы – не более 7 рабочих дней, включая обучение вашего персонала.

Простота эксплуатации

Интуитивно понятный и удобный интерфейс. Для установки и эксплуатации платформы не требуется наличие особых знаний.

Интеллектуальный WAF

Использование технологии машинного обучения после фильтрации трафика на уровнях L3–L7.

Клиентская поддержка

Оперативная и внимательная служба поддержки платформы локального офиса. В рабочее время поддерживаем прямую коммуникацию в мессенджерах.

Практичный дизайн

Еженедельно изучаем обратную связь от пользователей/администраторов платформы, использующих нашу систему, и вносим в нее улучшения.

Гибкое расширение лицензии

При возникновении в процессе эксплуатации системы потребностей в дополнительных ресурсах, не описанных в спецификации, можно быстро докупить необходимые мощности.

Отказоустойчивость

Система не перестает работать при отключении одного или нескольких компонентов за счет возможности построения отказоустойчивой сбалансированной архитектуры.

Оптимальная стоимость

Соотношение цена/качество системы находится на оптимальном уровне по сравнению с аналогами.

Адаптивность

Возможность разработки собственных правил безопасности и адаптации платформы под специфику конкретной компании.

Архитектура платформы

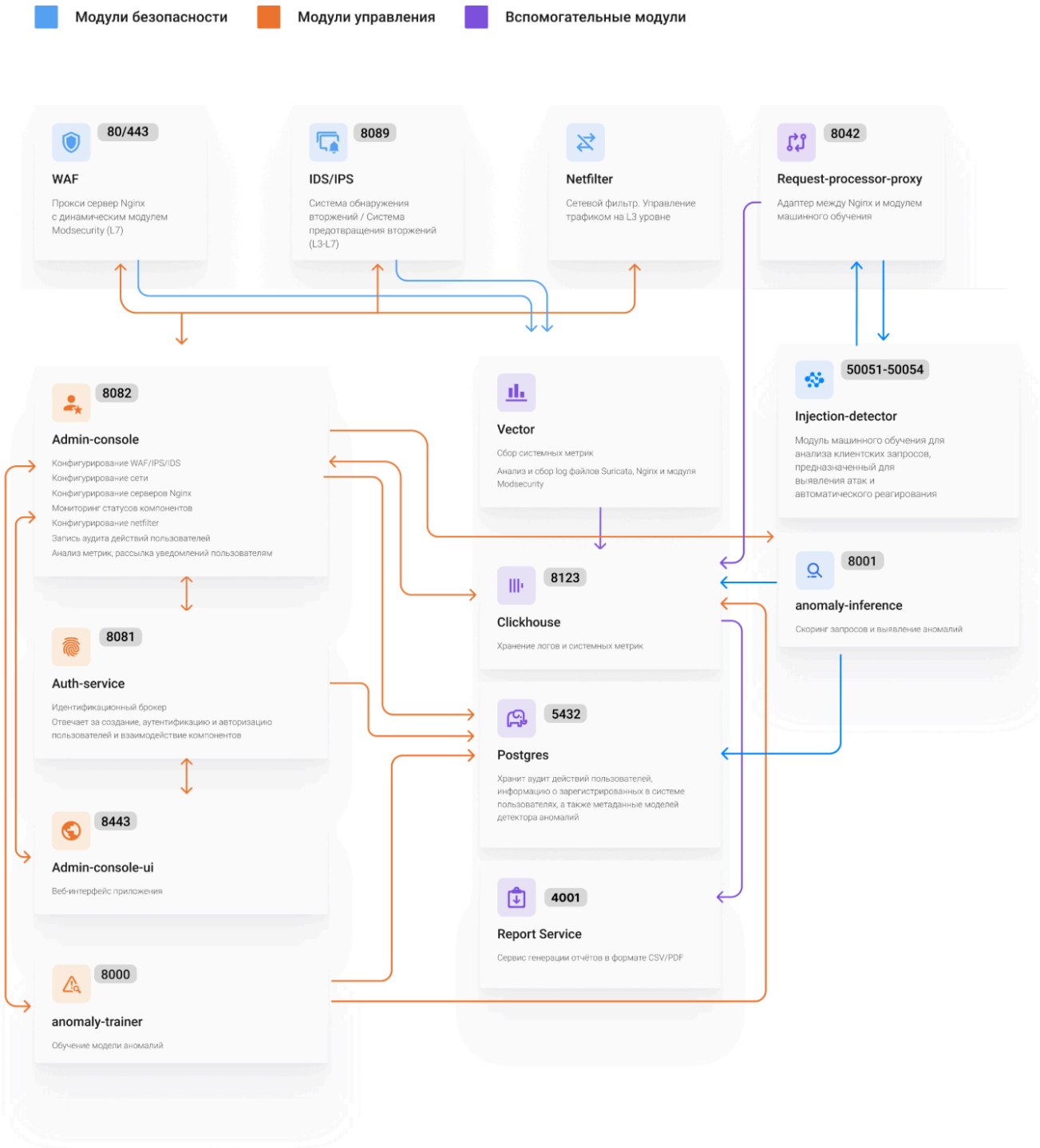
Frisbee WAF включает следующие функциональные модули:

- Анализатор – модуль, предназначенный для обнаружения возможных угроз, сопоставления их с базой знаний и блокирования, определения новых типов угроз и помещения их в базу знаний;
- База знаний – модуль, включающий набор правил с идентифицированными или определенными угрозами;
- Веб-интерфейс визуализации и управления – модуль, предназначенный для администрирования Frisbee WAF, работы в различных ролевых моделях, управления (добавления, удаления) пользователями, создания (редактирования, удаления) новых кастомных правил, просмотра и настройки метрик и др.

В основе архитектуры Frisbee WAF лежит сетевая модель OSI. Функциональные модули и компоненты сделаны с учетом обнаружения угроз и реагирования на них на следующих уровнях OSI:

L3 Сетевой уровень (network layer).
L4 Транспортный уровень (transport layer).
L5 Сеансовый уровень (session layer).
L6 Уровень представления (presentation layer).
L7 Прикладной уровень (уровень приложений; application layer).

Компоненты


Модули безопасности
Модули управления
Вспомогательные модули
80/443
WAF
Прокси сервер Nginx с динамическим модулем Modsecurity (L7)
8089
IDS/IPS
Система обнаружения вторжений / Система предотвращения вторжений (L3-L7)
Netfilter
Сетевой фильтр. Управление трафиком на L3 уровне
8042
Request-processor-proxy
Адаптер между Nginx и модулем машинного обучения
8082
Admin-console
Конфигурирование WAF/IPS/IDS
Конфигурирование сети
Конфигурирование серверов Nginx
Мониторинг статусов компонентов
Конфигурирование netfilter
Запись аудита действий пользователей
Анализ метрик, рассылка уведомлений пользователям
Vector
Сбор системных метрик
Анализ и сбор log файлов Suricata, Nginx и модуля Modsecurity
50051-50054
Injection-detector
Модуль машинного обучения для анализа клиентских запросов, предназначенный для выявления атак и автоматического реагирования
8123
Clickhouse
Хранение логов и системных метрик
8001
anomaly-inference
Скоринг запросов и выявление аномалий
8081
Auth-service
Идентификационный брокер
Отвечает за создание, аутентификацию и авторизацию пользователей и взаимодействие компонентов
5432
Postgres
Хранит аудит действий пользователей, информацию о зарегистрированных в системе пользователях, а также метаданные моделей детектора аномалий
8443
Admin-console-ui
Веб-интерфейс приложения
4001
Report Service
Сервис генерации отчётов в формате CSV/PDF
8000
anomaly-trainer
Обучение модели аномалий

Описание компонентов

Компонент	Описание
WAF	прокси-сервер Nginx с динамическим модулем ModSecurity (L7)
IDS/IPS	программный компонент на основе Suricata, предназначенный для обнаружения вторжений (Intrusion Detection System), предотвращения вторжений (Intrusion Prevention System) (L3-L7)
Netfilter	сетевой фильтр, компонент ядра Linux, обеспечивающий фильтрацию и управление сетевым трафиком
Admin Console	система менеджмента, предназначенная для конфигурирования и управления компонентами системы
Admin Console UI	веб-интерфейс системы менеджмента
Auth-service	идентификационный брокер, обеспечивающий создание, аутентификацию и авторизацию пользователей
Vector	модуль сбора и визуализации системных метрик
ClickHouse	хранение логов и системных метрик
Postgres	реляционная СУБД, предназначенная для хранения данных пользователей, аудита действий, метаданных моделей, а также метаданные моделей детектора аномалий
Report Service	вспомогательный компонент системы, предназначенный для формирования отчетов по результатам обработки данных, включая биллинговые отчеты, отчеты по метрикам и иную аналитическую информацию
Request-processor-proxy	адаптер между Nginx и модулем машинного обучения, обеспечивающий передачу запросов на анализ
Injection-detector	модуль машинного обучения для анализа клиентских запросов, предназначенный для выявления атак и автоматического реагирования
Anomaly-trainer	модуль обучения модели аномалий
Anomaly-inference	модуль скоринга запросов и выявления аномалий

Оперативная техническая поддержка локального офиса

Прием заявок по технической поддержке (e-mail)	**Обновление версии продукта** согласно планам разработки **Обновление базы правил** для ips/ids и waf	**Гарантированное время обработки запросов**	**Возможность создавать запросы** на добавление/ изменение функционально сти продукта	**Выделенный канал поддержки**	**Консультации** по уязвимостям, настройке правил, интеграции
Пакет Стандарт				09:00 -18:00 Пн-Пт	
Пакет Премиум				24/7	

Техническая поддержка осуществляется в зависимости от приобретенного пакета

Степени критичности инцидентов:

Критический – ошибки (баги) в работе ПО, влекущие прерывание (недоступность) информационных систем Заказчика для конечного пользователя

Существенный – ошибки (баги) в работе одного или нескольких компонентов ПО, влекущие ухудшение (нарушения) в работе информационных систем Заказчика

Незначительный – ошибки (баги) в работе одного или нескольких компонентов ПО, не влекущие ухудшение (нарушение) в работе информационных систем Заказчика

	Критический инцидент Макс. время реакции / время обработки	**Существенный инцидент** Макс. время реакции / время обработки	**Незначительный инцидент** Макс. время реакции / время обработки
Пакет Стандарт	2 часа / 2 дня	6 часов / 4 дня	12 часов / 12 дней
Пакет Премиум	1 час / 24 часа	2 часа / 2 дня	6 часов / 6 дней

Время реакции технической поддержки на запрос рассчитывается с момента получения запроса от Заказчика до первичного ответа специалиста с уведомлением о принятии запроса в работу (e-mail).

Время обработки запроса от Заказчика рассчитывается с момента отправки уведомления о принятии запроса в работу до предоставления инструкции по устранению проблемы либо классификации проблемы, указанной в запросе, как дефекта ПО. Дефект фиксируется в баг-трекинговой системе для устранения.