Программное обеспечение

«Servicepipe Cybert»

Описание функциональных характеристик программного обеспечения

Москва - 2026 г.

Содержание

1. О документе

Настоящий документ содержит описание функциональных характеристик программного обеспечения «Servicepipe Cybert» (далее - Servicepipe Cybert, Cybert, программное обеспечение, ПО). Документ предназначен для подтверждения назначения, состава и пользовательских возможностей программного обеспечения, включая функции защиты веб-ресурсов, анализа трафика, настройки политик, мониторинга и эксплуатации.

В документе используются следующие термины и определения:

Термин / Сокращение	Определение
Cybert	Программное обеспечение Servicepipe для защиты веб-ресурсов и приложений от вредоносного автоматизированного трафика и прикладных DDoS-атак.
Защита приложений	Верхнеуровневый раздел панели управления Servicepipe, в котором доступны ресурсы Cybert, статистика, аналитика, журналы, пользовательские правила, обнаруженные аномалии и пользовательские события.
Ресурс	Защищаемое веб-приложение или группа доменов, для которых задаются параметры интеграции, источники трафика и политики защиты.
Источник	Backend-сервер или иной узел Заказчика, к которому передаются разрешенные запросы.
Схема подключения	Способ интеграции ресурса с Cybert. В интерфейсе используются схемы «Прокси», «Модуль» и «Гибрид». Дополнительно ПО может поставляться в он-прем варианте.
Прокси	Схема, при которой входящий веб-трафик проходит через инфраструктуру фильтрации Servicepipe, после чего разрешенные запросы передаются на источник.
Модуль	Схема локальной интеграции с фронтенд-сервером NGINX/Angie, при которой метаданные запроса передаются Cybert, а итоговый вердикт применяется на стороне фронтенд-сервера.
Он-прем	Вариант поставки, при котором компоненты Servicepipe Cybert развертываются в инфраструктуре Заказчика. По набору доступных функций панели управления он аналогичен схеме «Модуль».
Гибрид	Схема, объединяющая облачную фильтрацию сетевого уровня и локальную обработку прикладного трафика средствами Cybert.
Класс источника	Результат классификации запроса: бот, вероятно бот, вероятно человек или человек.
JS score	Оценка, формируемая по результатам клиентской JavaScript-проверки и используемая в механизмах классификации.
Пользовательское правило	Настраиваемая политика ограничения интенсивности, выбора действия защиты, сбора JS score или классификации ботов.
Аномалия	Зафиксированный системой период нетипичного или вредоносного трафика с агрегированными показателями и аналитическими срезами.
RPS / RPM	Количество запросов в секунду / минуту.
ASN	Номер автономной системы источника трафика.
SNI	Имя сервера, передаваемое клиентом при установлении TLS-соединения.
Пользователь	Представитель Заказчика, которому предоставлен доступ к функциям Cybert через панель управления в соответствии с назначенными правами.

2. О программном обеспечении

Программное обеспечение «Servicepipe Cybert» предназначено для защиты веб-ресурсов и приложений от вредоносного автоматизированного трафика. ПО взаимодействует с фронтенд-серверами и компонентами приема входящего трафика, анализирует сетевые и прикладные параметры запросов, поведение пользователя в пределах сессии и дополнительные данные, получаемые на стороне клиента при выполнении проверок.

На основании совокупности доступных признаков Cybert формирует оценку вероятности автоматизированной активности и применяет настроенные правила разрешения, дополнительной проверки, ограничения интенсивности либо блокирования запросов. Основной функциональной особенностью ПО является автоматическое распознавание и блокирование вредоносного бот-трафика при сохранении доступа для легитимных пользователей и полезных автоматизированных клиентов.

В зависимости от архитектуры проекта Cybert может использоваться по схеме «Прокси», в локальной схеме «Модуль», в гибридной схеме либо в он-прем варианте поставки. Для он-прем поставки компоненты размещаются в инфраструктуре Заказчика, а набор доступных функций панели управления аналогичен схеме «Модуль».

Программное обеспечение обеспечивает, в частности:

- сигнатурный анализ сетевых и прикладных параметров входящих запросов;
- поведенческий анализ действий пользователя и последовательности запросов в пределах сессии;
- учет результатов JavaScript-, Cookie- и CAPTCHA-проверок;
- классификацию источников трафика и применение действий защиты;
- ограничение интенсивности запросов по URI и дополнительным условиям;
- формирование и применение пользовательских правил защиты;
- ведение белых и черных списков, а также географических ограничений;
- сбор статистики, аналитики, журналов запросов и данных по обнаруженным аномалиям;
- формирование пользовательских событий при пересечении заданных порогов метрик.

3. Информация о правообладателе

Параметр	Значение
Полное наименование	Общество с ограниченной ответственностью «Сервиспайп»
Сокращенное наименование	ООО «Сервиспайп»
ИНН	7708257951
КПП	772201001
ОГРН	1157746483784
Юридический адрес	Россия, 111024, г. Москва, ул. Кабельная 2-я, д. 2, стр. 3, эт. 2, помещение XVIII, ком. 8
Телефон	+7 (495) 374-62-65
Адрес электронной почты	welcome@servicepipe.ru
Веб-сайт	servicepipe.ru

4. Функциональные возможности

Состав доступных функций Cybert определяется схемой подключения или вариантом поставки, конфигурацией учетной записи, ролью Пользователя и назначенными правами. Основные пользовательские функции доступны в разделе «Защита приложений» панели управления Servicepipe.

4.1 Общие сведения

Панель управления предоставляет единую модель работы с защищаемыми ресурсами. Пользователь может создавать и удалять ресурсы, изменять настройки интеграции и защиты, просматривать статистику и журналы, настраивать пользовательские правила и анализировать зафиксированные системой события.

- табличный просмотр ресурсов и связанных сущностей с поиском, фильтрами, пагинацией и меню действий;
- создание и редактирование объектов через формы с обязательными полями, переключателями, выпадающими списками, множественным выбором и списками условий;
- валидация значений при сохранении, включая адреса, подсети, домены, сроки действия, числовые лимиты и обязательные параметры;
- разграничение доступных функций в зависимости от роли пользователя и состава подключенных возможностей;
- подтверждение необратимых операций и отображение результата выполнения действий в интерфейсе.

4.2 Управление защищаемыми ресурсами и схемами подключения

ПО поддерживает создание и сопровождение защищаемых веб-ресурсов. При создании задаются имя ресурса и схема подключения. В интерфейсе доступны схемы «Прокси», «Модуль» и «Гибрид»; он-прем является отдельным вариантом поставки, для которого набор функций панели управления аналогичен схеме «Модуль».

- просмотр списка ресурсов с идентификатором, именем или доменом, сервисным IP и доступными действиями;
- создание ресурса и выбор схемы подключения;
- переход к обзору, статистике, аналитике, логам, пользовательским правилам и настройкам выбранного ресурса;
- изменение имени и описания ресурса;
- очистка кэша ресурса при наличии соответствующей функции;
- удаление ресурса после подтверждения;
- поддержка прокси-схемы с передачей разрешенных запросов на источник;
- поддержка локальной интеграции с NGINX/Angie по схеме «Модуль»;
- поддержка гибридной схемы, объединяющей облачную сетевую защиту и локальную обработку L7-трафика;
- поддержка он-прем поставки с размещением компонентов Cybert в инфраструктуре Заказчика.

4.3 Управление основными настройками ресурса

Вкладка «Основные настройки» содержит идентификационные параметры ресурса и базовые переключатели обработки трафика. Набор доступных параметров зависит от схемы интеграции и варианта поставки.

- задание имени и текстового описания ресурса;
- включение механизмов защиты от DDoS-атак на уровне приложений;
- управление доступом для распознанных поисковых роботов;

- включение перенаправления HTTP-запросов на HTTPS;
- настройка схемы передачи разрешенных запросов на источник;
- включение перенаправления с домена с префиксом www на основной домен без префикса;
- сохранение изменений с последующим применением конфигурации к выбранному ресурсу.

4.4 Управление доменами и SSL-сертификатами

ПО поддерживает настройку доменных имен защищаемого ресурса и сертификатов, используемых для TLS-соединений. Для ресурса может быть определен основной домен и дополнительные домены-алиасы.

- просмотр состояния и срока действия основного сертификата;
- использование автоматического выпуска и продления сертификата Let’s Encrypt при наличии соответствующей функции;
- загрузка или замена цепочки сертификатов в формате PEM;
- загрузка приватного RSA-ключа в формате PEM;
- добавление защищаемых доменов и доменов-алиасов;
- использование основного сертификата для алиаса, если сертификат покрывает соответствующее имя;
- загрузка отдельного сертификата для домена-алиаса;
- удаление домена-алиаса после подтверждения.

4.5 Управление источниками и отказоустойчивостью

Для прокси-сценариев ПО позволяет задавать один или несколько backend-источников, на которые передаются разрешенные запросы. Источникам назначаются режим, вес и параметры временного исключения при ошибках.

- добавление источника по IPv4-адресу;
- выбор режима «Основной», «Резервный» или «Отключён»;
- назначение веса для распределения трафика между источниками одинакового режима;
- ведение описания источника;
- настройка порога ошибок, после которого источник временно исключается из обработки;
- настройка времени отключения источника после достижения порога ошибок;
- редактирование параметров источника и вывод неиспользуемых узлов из эксплуатации.

4.6 Управление белыми, чёрными списками и геоограничениями

ПО предоставляет механизмы явного управления доверенными и блокируемыми IP-адресами и подсетями, а также ограничения доступа по географическому признаку.

- добавление IPv4-адресов и подсетей в белый список с описанием и необязательным сроком действия;
- добавление IPv4-адресов и подсетей в черный список с описанием и необязательным сроком действия;
- массовое добавление до 2000 адресов за одну операцию и ведение списков объемом до 60 000 адресов;
- поддержка частичного результата массового добавления с сохранением корректных значений и отображением ошибок по некорректным;
- редактирование описания и срока действия существующей записи;
- удаление записей из списков;
- режим геоограничений «Без ограничений»;
- режим «Разрешить выбранные страны»;

• режим «Заблокировать выбранные страны» с множественным выбором стран.

4.7 Анализ запросов, классификация и действия защиты

Cybert анализирует совокупность признаков запроса и сессии, формирует оценку автоматизированной активности и определяет класс источника. Для принятия решения могут учитываться сетевые, транспортные, TLS-, HTTP-, поведенческие и клиентские признаки.

- анализ IP-адреса и подсети, ASN, географического признака и принадлежности к хостинговой или анонимизирующей инфраструктуре;
- анализ версии протокола, TLS-параметров, наборов шифров, расширений и сервисных отпечатков;
- анализ HTTP-метода, Host, URL-пути, Query string, Referer, User-Agent, заголовков, Cookie, Content-Type и версии HTTP;
- учет последовательности запросов, частоты и временных интервалов, переходов между страницами и признаков новой сессии;
- учет результатов JavaScript-, Cookie- и CAPTCHA-проверок;
- классификация трафика по категориям «Бот», «Вероятно бот», «Вероятно человек» и «Человек»;
- применение действий «По умолчанию», «Пропустить», «Блокировать», JS-проверка, Cookie-проверка и CAPTCHA;
- учет состояния прикладной DDoS-атаки при выборе правил и действий.

4.8 Статистика и мониторинг защищаемого ресурса

ПО поддерживает просмотр агрегированной статистики и временных графиков за выбранный период. Пользователь может использовать быстрые интервалы и произвольные диапазоны в пределах ограничений соответствующего раздела.

- обзор действий защиты и соотношения разрешенных, заблокированных и направленных на проверку запросов;
- распределение трафика по классам источников;
- просмотр входящей, исходящей, пропущенной и заблокированной полосы;
- просмотр статистики CAPTCHA: выдано, успешно решено, разрешено после CAPTCHA;
- просмотр времени ответа источника и общего времени обработки;
- просмотр кодов ответа источника по классам 2xx, 3xx, 4xx и 5xx;
- детализация ошибок источника 500, 501, 502, 503 и 504;
- просмотр кодов ответа платформы защиты по классам 2xx, 3xx, 4xx и 5xx;
- просмотр географических и доступных TCP-метрик;
- включение и скрытие отдельных серий графиков, просмотр точных значений при наведении и обновление данных.

4.9 Аналитика источников и структуры трафика

Раздел «Аналитика» предоставляет распределения и топы по ключевым измерениям. Максимальный период анализа в пользовательском интерфейсе составляет 31 день.

- фильтрация аналитики по действию защиты;
- фильтрация по классу источника;
- фильтрация по причине действия;
- анализ наиболее активных IP-адресов и подсетей;
- анализ наиболее часто запрашиваемых URL-путей;
- анализ User-Agent и клиентских характеристик;
- анализ распределения по странам;
- анализ ASN и сетевых владельцев;

• переход от агрегированных значений к детализации в журнале запросов.

4.10 Журналы запросов, поиск и экспорт

ПО поддерживает поиск и исследование отдельных запросов в разделе «Логи запросов». В интерфейсе доступны журнал всего трафика и журнал запросов, для которых оценивались или применялись политики защиты. Доступный период хранения в интерфейсе - последние две недели.

• поиск по ID запроса и ID сессии;
• фильтрация по User-Agent, IP источника, Host, Referer, HTTP-методу, пути и Query string;
• фильтрация по стране, схеме, версии HTTP и сетевым атрибутам;
• фильтрация по классу источника, действию, причине и ID правила;
• просмотр сервисных отпечатков, JA3, типа запроса и Bot score при наличии данных;
• просмотр кода ответа клиенту и кода ответа источника;
• просмотр IP и порта backend-источника, времени ответа источника и общего времени запроса;
• открытие подробной карточки отдельного запроса;
• экспорт журнала за интервал не более 24 часов;
• отправка сформированной выгрузки на указанный адрес электронной почты;
• отображение до 10 000 записей в результате пользовательского запроса к таблице журнала.

4.11 Ограничение интенсивности запросов

ПО поддерживает отдельные правила «Лимиты запросов» для ограничения частоты обращений к одному или нескольким URI. При превышении заданного порога источник может быть временно заблокирован.

• создание именованного правила ограничения интенсивности;
• задание одного или нескольких URI;
• использование операторов точного совпадения и совпадения по началу пути;
• объединение нескольких URI внутри правила по логике «ИЛИ»;
• настройка максимально допустимого количества запросов;
• настройка периода подсчета до 86400 секунд;
• настройка времени временной блокировки до 86400 секунд;
• включение и отключение правила без удаления его конфигурации.

4.12 Пользовательские правила защиты

«Правила защиты» позволяют описывать гибкие условия сопоставления трафика, учитывать лимиты и состояние DDoS-атаки, а затем назначать действия для соответствующих классов источников. Правила обрабатываются последовательно; применяется первое подходящее правило.

• управление позицией правила в последовательности обработки;
• задание описания и состояния правила;
• условия по стране, ASN, Query string, URL-пути и сегменту пути;
• условия по Content-Type, Cookie, HTTP-заголовкам, Host, методу, Referer и User-Agent;
• условия по IP-адресам и подсетям, X-Forwarded-For, хостинговой инфраструктуре, сервисным хэшам и признаку нового пользователя;
• операторы «Входит в», «Не входит в», «Равно», «Не равно», «Содержит», «Не содержит», «Начинается с», «Заканчивается на», «Пустое», «Не пустое» и другие поддерживаемые варианты;
• общий лимит запросов и отдельный лимит для IP-адреса;
• периоды лимита 1 секунда, 10 секунд, 1 минута, 5 минут и 10 минут;
• применение действия до либо после превышения лимита;

- режимы действия правила «Всегда», «Пока нет атаки» и «Во время атаки»;
- назначение отдельного действия для классов «Бот», «Вероятно бот», «Вероятно человек» и «Человек»;
- поддержка действий пропуска, блокирования, JS-проверки, Cookie-проверки и CAPTCHA с уровнями сложности;
- изменение порядка, включение, отключение, редактирование и удаление правил.

4.13 Специальное правило защиты API

Cybert поддерживает специальное правило защиты API для endpoint-ов, которые должны вызываться в рамках пользовательского веб-сценария. Запрос к защищаемому API разрешается при наличии подтвержденного предварительного посещения веб-страницы ресурса в течение заданного времени.

- создание не более одного специального правила защиты API для одного ресурса;
- фиксированный приоритет обработки перед обычными правилами защиты;
- настройка одного или нескольких защищаемых URL-путей;
- операторы точного совпадения и совпадения по началу пути;
- настройка разрешенного времени после посещения веб-страницы;
- готовые интервалы от 5 минут до 24 часов;
- пользовательское значение времени до 1440 минут;
- включение и отключение специального правила.

4.14 Сбор JS score и классификация ботов

ПО поддерживает управляемый сбор клиентских признаков через JavaScript и последующую классификацию по значению JS bot score.

- создание правил «Сбор JS score» с позицией, описанием, условиями трафика, состоянием DDoS и признаком включения;
- выдача JavaScript только для областей трафика, в которых браузер может корректно выполнить клиентский сценарий;
- использование условий, аналогичных правилам защиты, для ограничения области сбора;
- использование полученного JS score в дальнейшей классификации и механизмах защиты;
- создание общих и условных правил «Классификация ботов»;
- настройка порога Bot score в диапазоне от 0 до 1 с шагом 0,1;
- применение наиболее строгого, то есть минимального, порога при одновременном совпадении нескольких включенных правил;
- включение, отключение, редактирование и удаление правил классификации.

4.15 Обнаруженные аномалии

Раздел «Обнаруженные аномалии» содержит периоды нетипичного или вредоносного трафика, зафиксированные системой для защищаемых ресурсов. Функция используется для ретроспективного анализа атаки и сопоставления структуры трафика с действиями защиты.

- просмотр списка аномалий с ID, временем начала и окончания, ресурсом, максимальной скоростью блокировок и суммарным количеством заблокированных запросов;
- фильтрация списка по периоду, ресурсу и идентификатору;
- просмотр карточки аномалии со сводкой и временной динамикой запросов;
- распределение действий защиты и классов источников в период аномалии;
- аналитические топы по странам, IP-адресам, подсетям, URL-путям, User-Agent и определенным операционным системам;

• сопоставление аномалии с журналами запросов и пользовательскими правилами.

4.16 Пользовательские события

Функция «Пользовательские события» позволяет задавать порог по выбранной метрике и фиксировать периоды, когда значение становится больше или меньше заданного порога.

• выбор защищаемого ресурса, для которого контролируется метрика;
• выбор типа метрики и конкретного показателя;
• условия «Больше» и «Меньше»;
• выбор единицы измерения, включая Кбит/с и Мбит/с для полосы, RPS и RPM для количества запросов;
• задание числового порога;
• контроль входящей, исходящей, разрешенной и заблокированной полосы;
• контроль действий над запросами, включая блокирование, пропуск, перенаправление и дополнительные проверки;
• контроль статистики CAPTCHA;
• контроль классов HTTP-кодов платформы и источника;
• контроль общего времени обработки и времени ответа источника;
• контроль классов источников и отдельных ошибок источника 5xx;
• просмотр списка условий и зафиксированных срабатываний.

4.17 Дополнительные клиентские проверки

Cybert может использовать дополнительные клиентские проверки в ситуациях, когда имеющихся признаков недостаточно для однозначного решения. Проверки помогают подтвердить способность клиента выполнять браузерный сценарий и уточнить классификацию.

• JS-проверка с уровнями «Простой», «Обычный» и «Сложный»;
• Cookie-проверка способности клиента получить и вернуть служебную cookie;
• CAPTCHA с уровнями «Простой», «Продвинутый» и «Сложный»;
• назначение проверки системным профилем защиты или пользовательским правилом;
• применение проверки в зависимости от состояния DDoS-атаки;
• повторная проверка при отсутствии требуемой служебной cookie или необходимости обновления результата;
• использование JS score и других признаков для принятия решения о дополнительной проверке.