|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| wordml://2.png | |  |  | | --- | --- | |  |  | | wordml://4.png | | | **Программный комплекс** | | | SolarCloud | | | wordml://5.png | | | Версия 1.0.0 | | | wordml://6.png | | | **Руководство по администрированию** | | | Москва, 2024 | | | wordml://8.png |
| wordml://9.png | |  |

Оглавление

[Оглавление 2](#_Toc165042398)

[Аннотация 3](#_Toc165042399)

[Перечень сокращений 4](#_Toc165042400)

[1. Сведения о SolarCloud 5](#_Toc165042401)

[1.1. Назначение и основные возможности SolarCloud BotShield 5](#_Toc165042402)

[1.2. Архитектура SolarCloud BotShield 6](#_Toc165042403)

[1.3. Алгоритм работы SolarCloud BotShield 7](#_Toc165042404)

[2. Описание административного интерфейса SolarCloud 9](#_Toc165042405)

[2.1. Отображение вердикта модуля 9](#_Toc165042406)

[2.2. Описание основных элементов платформы 9](#_Toc165042407)

[3. Описание блока команд для установки модуля 10](#_Toc165042408)

[3.1. Описание установки BotShield на операционную систему Debian 12 10](#_Toc165042409)

[3.2. Настройка конфигурационного фала nginx 11](#_Toc165042410)

[3.3. Выполнение запроса 11](#_Toc165042411)

[3.4. Просмотр событий фала лога 11](#_Toc165042412)

[4. Получение технической поддержки 12](#_Toc165042413)

[Лист контроля версий 13](#_Toc165042414)

Аннотация

Настоящий документ представляет собой руководство по администрированию программного комплекса «SolarCloud» (далее – SolarCloud). Документ предназначен для администраторов BotShield и содержит описание процедур настройки модуля.

Перечень сокращений

АРМ Автоматизированное рабочее место

БД База данных

BS BotShield модуль

OC Операционная система

ПО Программное обеспечение

ПК Программный комплекс

СУБД Система управления базами данных

IdM Identity Management

GUI Graphical User Interface – графический интерфейс пользователя

AGUI Веб-интерфейс администратора Solar inRights

CLI Command Line Interface – интерфейс командной строки

УЗ Учетная запись

1. Сведения о SolarCloud
   1. Назначение и основные возможности SolarCloud BotShield

**SolarCloud** — Это программный комплекс класса облачной платформы, который включает в себя подсистемы и сервисы для анализа и фильтрации трафика к веб ресурсу. Платформа SolarCloud включает подсистему анализа клиентских сессий - BotShield. Некоторые алгоритмы шифрования характерны для браузеров, другие - для библиотек, позволяющих выполнять автоматизированные запросы. Модуль BotShield представляет собой программное обеспечение, предназначенное для оценки клиентских сессий веб-сайтов и интернет-ресурсов от вредоносных ботов и автоматизированных атак. Применение такой системы имеет ряд значительных преимуществ и помогает решить множество задач по обеспечению безопасности. Ключевое назначение подсистемы BotShield:

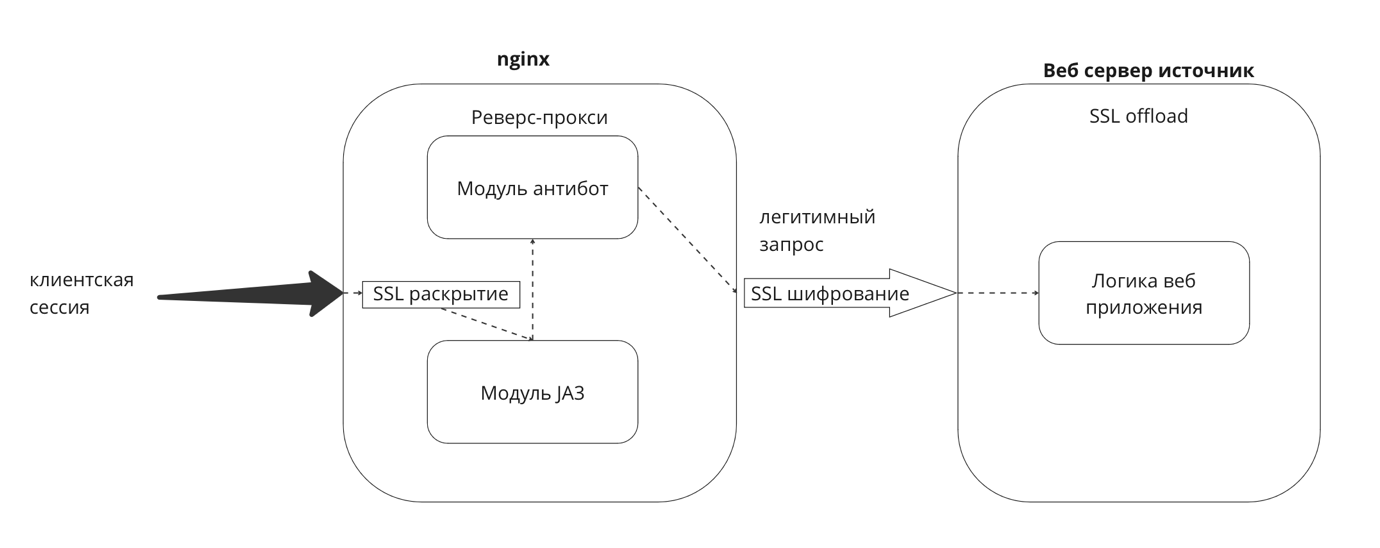
1. Оценка трафика. На основе анализа характеристик запросов, таких как IP-адреса, заголовки HTTP, поведение пользователей и др., система оценивает весь трафик, и делает финальный вердикт каждого запроса с идентификатором от 0 до 100. На основании данного вердикта выставляется значение, при котором сессия будет заблокирована.
2. Защита от DDoS-атак. Модуль BotShield применяется для борьбы с распределенными атаками типа "отказ в обслуживании" (DDoS), при которых злоумышленники используют ботнеты для генерации огромного количества запросов к ресурсу с целью его перегрузки и выведения из строя.
3. Уменьшение нагрузки на инфраструктуру. Путем отсеивания ботов и нежелательного трафика система помогает уменьшить нагрузку на сервера и инфраструктуру веб-сайта, что важно для поддержания высокой производительности и доступности сервера-оригинатора для пользовательских легитимных запросов.
4. Защита от скрапинга. Автоматизированные скрипты или боты часто используются для нелегального сбора данных с веб-сайтов (скрапинг). Облачная система предотвращает кражу контента и данных пользователей, распознавая попытки скрапинга.
5. Снижение риска фрода. Боты могут использоваться для проведения фродовых операций, таких как автоматизированное создание фейковых аккаунтов, выполнение сомнительных финансовых операций или манипуляции с онлайн-голосованиями.
6. Повышение точности аналитики. Нежелательный бот-трафик может искажать аналитические данные веб-сайта, такие как статистика посещаемости, поведение пользователей и конверсия. Отсеивание ботов помогает поддерживать точность аналитической информации, что важно для эффективного управления ресурсом.
7. Улучшение пользовательского опыта. Защита от вредоносных ботов помогает обеспечить стабильную и быструю работу ресурса, что напрямую влияет на удовлетворенность и лояльность пользователей.

Система работает с большим количеством данных и параметров для того, чтобы вынести максимально корректный вердикт. Модуль оценивает набор алгоритмов клиента и выносит вердикт, насколько характерен данный набор для автоматизированного бота. На основании данного вердикта выставляется значение, при котором сессия будет заблокирована.

* 1. Архитектура SolarCloud BotShield

SolarCloud построен с использованием модульной архитектуры и состоит из следующих компонентов:

* **Реверс-прокси** — в качестве реверс-прокси сервера выполняет терминирование запросов и предоставляет дополнительный уровень безопасности с помощью таких функций, как SSL-терминация (расшифровка SSL-запросов перед тем, как они достигнут приложения и пройдут через модуль).
* **Модуль JA3** — высокопроизводительный модуль nginx для отпечатков клиентских сессий ja3 и http2.
* **Модуль оценки клиентских сессий BotShield** — Этот модуль анализирует входящий трафик и принимают решение о том, разрешать запрос или блокировать его, основываясь на наборе предопределённых правил и алгоритмах. Модуль проверяет заголовки HTTPS запросов на предмет подозрительных или аномальных значений, которые часто используются ботами, например, отсутствие заголовков «User-Agent», «Referer», или использование необычных значений.
* Схема архитектуры SolarCloud антибот приведена на [**Рис.1.1**](#ris_architect).



**Рис. 1.1. Архитектура SolarCloud BotShield (https запрос)**

При установлении защищенного соединения между клиентом и сервером происходит процесс SSL/TLS рукопожатия, в ходе которого обмениваются сертификаты и зашифрованные ключи. NGINX на этом этапе должен расшифровать трафик, являться звеном где терминируется SSL/TLS трафик, чтобы антибот-модуль мог провести анализ содержимого HTTPS-запросов. Это необходимо, поскольку основные параметры анализа не доступны в зашифрованном виде.

**Примечание**

*Модуль BotShield работает как фильтрующий элемент клиентских сессий.*

BotShield модуль анализирует множество параметров, включая, но не ограничиваясь: заголовки HTTP, IP-адреса, частоту запросов, поведенческие характеристики пользователей. Этот анализ позволяет собрать достаточно данных для принятия решения о том, является ли посетитель ботом. На основе собранной аналитики система использует алгоритмы, с возможностью машинного обучения для определения вероятности того, что трафик исходит от бота. Этот результат представлен в виде процентного соотношения. В зависимости от пороговых значений, заранее настроенных администратором системы, BotShield-модуль принимает решение об обработке запроса: блокировать его, требовать дополнительную аутентификацию или пропускать.

**Примечание**

*Модуль работает со статическим набором параметров, которые анализируются внутри запущенного модуля.*

Функциональность обеспечивается добавлением в конфигурацию NGINX специфических директив, относящихся к антибот-модулям, и настройка этих модулей для использования JA3 хэшей, анализа поведенческих параметров и других признаков для детекции ботов. Модули могут логировать анализируемые запросы, что позволяет администраторам в дальнейшем тонко настраивать систему антибот-защиты.

Антибот-модуль для NGINX, использующий раскрытие SSL/TLS сертификатов, JA3-аналитику и комплексную проверку параметров запроса, предоставляет функционал для оценки и блокировки вредоносного бот-трафика, при этом минимизируя риски неправильной блокировки легитимных пользователей.

* 1. Алгоритм работы SolarCloud BotShield

Этап 1: Запрос от клиента к NGINX

1. Инициация Соединения: Клиент (браузер пользователя или потенциальный бот) отправляет HTTPS запрос к веб-сайту.
2. Прохождение через Интернет: Запрос проходит через различные сегменты сети Интернета, включая маршрутизаторы и шлюзы, до достижения NGINX сервера на котором будет происходить фильтрация.
3. SSL/TLS Рукопожатие: NGINX выполняет SSL/TLS рукопожатие с клиентом. Этот этап включает обмен ключами и сертификатами для установления зашифрованного соединения.
4. Расшифровка Трафика: NGINX расшифровывает полученные HTTPS запросы для последующего доступа к содержимому.

Этап 2: Анализ запроса на NGINX

1. Анализ JA3 Хэшей: NGINX использует хэши JA3 для анализа отпечатков TLS, позволяя идентифицировать уникальные параметры рукопожатия клиента.
2. Проверка Параметров Запроса: Антибот-модуль анализирует заголовки HTTP, IP-адреса, частоту запросов и другие параметры, чтобы определить, является ли входящий запрос от бота.
3. Определение Вероятности Бота: На основе собранных данных, NGINX с помощью антибот-модуля применяет алгоритмы для расчета вероятности того, что запрос исходит от бота.

Этап 3: Принятие Решения

1. Решение о Блокировке или Пропуске: Отправка значения в модель происходит через прямое взаимодействие с предобученной моделью машинного обучения. Модель машинного обучения, получив значения JA3 и JA3 хэшей, оценивает и возвращает вероятность того, что данный запрос является ботовым. Это происходит путём отправки запроса к сервису с отдельной переменной, где работает модель, с последующим анализом ответа, который будет включать оценку принадлежности запроса к ботовой, обрабатывать запрос как легитимный или как потенциально вредоносный. В зависимости от рассчитанной вероятности и предварительно установленных порогов, запрос может быть либо заблокирован, либо пропущен дальше.

Этап 4: Передача Обработанного Запроса

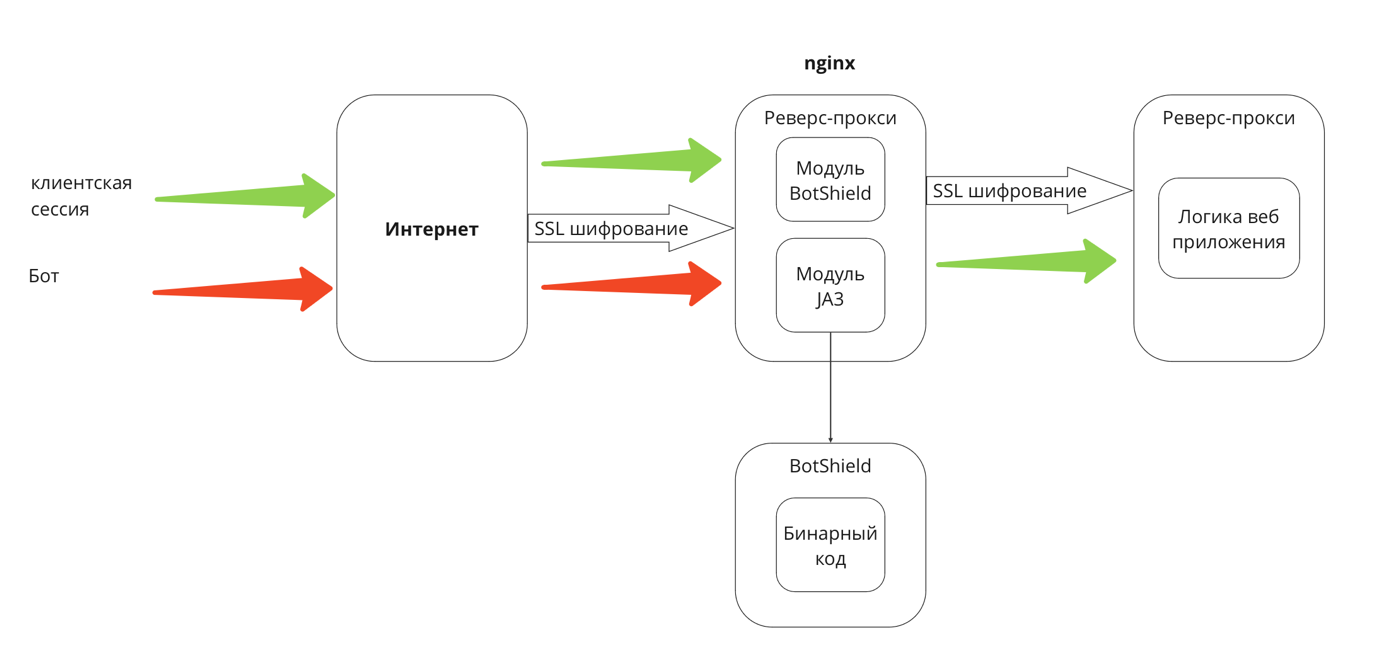
1. Перенаправление на Целевой Сервер: Если запрос одобрен, NGINX перенаправляет его на целевой веб-сервер с приложением.
2. Обработка Запроса: Целевой сервер обрабатывает запрос и генерирует соответствующий ответ.
3. Отправка Ответа клиенту: Ответ пересылается обратно клиенту через NGINX, возможно, снова используя SSL/TLS для шифрования данных.

Этап 5: Получение Ответа Клиентом

1. Расшифровка и Просмотр: Клиент получает, расшифровывает (при необходимости) и просматривает ответ от сервера.

В этом процессе ключевую роль играют SSL/TLS рукопожатие и анализ отпечатков TLS через JA3 хэши для идентификации клиентов, а также комплексный анализ параметров запроса для выявления и блокировки потенциальных ботов. Это позволяет эффективно защищать веб-приложения от различных вредоносных атак, минимизировать риски нарушения работы сервиса и обеспечивать безопасность данных пользователей.

* Схема взаимодействия SolarCloud и клиента приведена на **[Рис. 1.2.](#_Hlk165041675" \s "1,11710,11720,0,,Рис. 1.2. )**

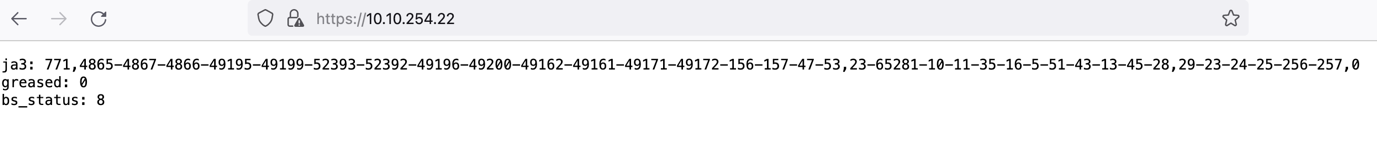


**Рис. 1.2. Схема процесса взаимодействия обработки запроса с кодом модели**

1. Описание административного интерфейса SolarCloud
   1. Отображение вердикта модуля

В локальном браузере будет отображен вердикт с присвоением процентного значения и принадлежностью запроса к ботовому, статус ml обозначает процент от 1 до 100

Отпечаток ja3 для данного запроса, greased: 0, вердикт модели **bs\_status: 8**



* 1. Описание основных элементов платформы

Модуль BotShield предназначен для анализа и оценки клиентских сессий. В первую очередь необходимо на вашем веб сервере Nginx настроить необходимый веб ресурс, входящие клиентские сессии которого нужно проанализировать. В случае отсутствия данного ПО (nginx) на рабочей ноде, - его необходимо установить.

Nginx — это высокопроизводительный веб-сервер и обратный прокси-сервер, который используется для масштабируемых веб-приложений. Его функционал включает в себя обработку статических данных, балансировку нагрузки, кэширование, а также возможность терминирования клиентских соединений и SSL раскрытие.

**Терминирование клиентских веб ресурсов**

Терминирование клиентских веб-соединений в контексте Nginx представляет процесс приема входящих клиентских запросов (обычно HTTP или HTTPS) и завершения этих соединений, передавая запросы к соответствующим серверам приложений или ресурсам. Это позволяет Nginx работать как точка входа в систему, где он может обрабатывать базовые задачи перед тем, как переслать запрос на бэкенд. Эти задачи включают в себя:

* Аутентификацию и авторизацию пользователей.
* Логирование запросов для сбора статистики.
* Манипуляции с запросами, такие как редиректы или изменение заголовков.
* Балансировку нагрузки между несколькими серверами приложений.

**SSL Offload**

SSL Offload относится к процессу снятия нагрузки, связанной с шифрованием и дешифрованием данных SSL/TLS, с серверов приложений на Nginx. Это позволяет серверам приложений сосредоточиться на своих основных задачах, увеличивая тем самым общую производительность системы. Процесс SSL offload включает:

1. Декодирование данных. Nginx принимает зашифрованные HTTPS-запросы от клиента, расшифровывает их используя сертификаты SSL/TLS, и пересылает декодированный HTTP-запрос на внутренний сервер или приложение.
2. Шифрование ответов. После обработки запроса на бэкенде, Nginx получает от него ответ, который затем шифруется и отправляется обратно клиенту по HTTPS.
3. Описание блока команд для установки модуля
   1. Описание установки BotShield на операционную систему Debian 12

Предварительно у вас должны быть установлены следующие пакеты:

libc-bin libxgboost-dev xgboost

Для того, чтобы их установить, вам необходимо запустить следующую команду:

apt install -y libc-bin libxgboost-dev xgboost

Скачайте файл .deb пакета с указанной ссылки и введите пароль (ссылка).

Для того, чтобы установить пакет, необходимо перейти в каталог где располагается скаченный файл и запустить следующую команду:

apt install -y ./nginx\_1.24.0-1~bookworm\_amd64.deb

После чего необходимо запустить установленное приложение командой:  
systemctl start nginx

* 1. Настройка конфигурационного фала nginx

Необходимо перейти в директорию /etc/nginx/conf.d/

Открыть файл bs\_test.conf

Раскомментировать все строки.

Далее необходимо вставить в строки 7 и 8 сертификаты для домена, который будет поставлен под защиту.

Директивы, в которых необходимо передать данные о сертификатах:

ssl\_certificate\_key ;

ssl\_certificate ;

На строке 4 при необходимости можно поменять значение вердикта необходимое для сброса клиентского запроса:

bot\_threshold 80;

* 1. Выполнение запроса

Для того, чтобы получить статус вердикта необходимо выполнить запрос до настроенного ресурса https в браузере или curl запросом.  
После чего будет отображен вердикт данного запроса

ja3: 771,4865-4866-4867-49196-49195-52393-49200-49199-52392-49162-49161-49172-49171-157-156-53-47-49160-49170-10,23-65281-10-11-16-5-13-18-51-45-43-27-21,29-23-24-25,0

greased: 1

bs\_status: 62

* 1. Просмотр событий фала лога

Для того, чтобы посмотреть последние 10 строк лога тестового ресурса необходимо выполнить следующую команду:

tail /var/log/nginx/bs\_test\_access.log

1. Получение технической поддержки

Контакты технической поддержки

Для получения консультации по техническим вопросам можно обратиться по адресу [**support@rt-soalar.ru**](mailto:support@rt-soalar.ru).

С условиями поддержки можно ознакомиться на сайте компании (по адресу: [**http://rt-solar.ru/support/**](http://rt-solar.ru/support/)). При оформлении запроса следует указать номер контракта на техническую поддержку, описать проблему, указать свое полное имя, адрес электронной почты и номер телефона.

Лист контроля версий

26/04/2024-13:46