ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«F6 Preventive Proxy»

Руководство по эксплуатации

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	**Описание**
АС	Автоматизированная система АО «БУДУЩЕЕ»
Бэкенд	Серверная часть веб- или мобильного приложения, отвечающая за обработку запросов от Пользователей, работу с базами данных и бизнес-логику
Заказчик	Лицо, которое использует на законных основаниях ПО на основании заключенного договора
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО «БУДУЩЕЕ»; • Компанией-интегратором, по выбору Заказчика
Ноды (nodes)	Также узлы; физические или виртуальные машины, на которых разворачиваются и запускаются контейнеры с приложениями в платформе Kubernetes
ПО	Программное обеспечение «F6 Preventive Proxy»
Прокси-сервер	Сервер (комплекс программ) в компьютерных сетях, выполняющий роль посредника между пользователем и целевым сервером (при этом о посредничестве могут как знать, так и не знать обе стороны). Позволяет клиентам как выполнять косвенные запросы (принимая и передавая их через прокси-сервер) к другим сетевым службам, так и получать ответы
Разработчик	АО «БУДУЩЕЕ»
Файл cookie	Файл с небольшим набором данных, которые веб-ресурс отправляет на компьютер пользователя для идентификации устройства

Фронтенд	Пользовательский интерфейс веб- или мобильного приложения, с которым взаимодействует Пользователь
Mobile SDK (далее – SDK)	Модуль программного обеспечения «F6 Fraud Protection» для встраивания в мобильные приложения
RSA	Криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших полупростых чисел
Web Snippet (далее – скрипт)	Модуль программного обеспечения «F6 Fraud Protection» для встраивания в WEB приложения

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит руководство по эксплуатации программного обеспечения «F6 Preventive Proxy» (далее — ПО, F6 Preventive Proxy, Preventive Proxy).

1.2 Назначение ПО

«F6 Preventive Proxy» — программное обеспечение для обнаружения интеллектуальных автоматизированных программ (ботов) и защиты от них, а также для снижения прямых убытков и издержек от мошеннической активности на веб-порталах и в мобильных приложениях (далее – АС Заказчика), которая происходит с использованием автоматизированных действий. В ПО используются машинное обучение и нейронные сети для анализа сессионных данных, экспертные скоринговые модели, анализ трафика, графовый анализ связанных ресурсов.

Preventive Proxy является подсистемой ПО «F6 Fraud Protection», которую можно использовать отдельно или с другими подсистемами продукта, комплексно защищая веб- или мобильное приложение и его пользователей от мошенничества.

1.3 Функциональные возможности ПО

Функциональные возможности «F6 Preventive Proxy»:

- Проверяет легитимность Пользователя и его окружение;
- Выявляет и защищает веб- и мобильные приложения от такой вредоносной бот-активности, как скрапинг, брутфорс, кража аккаунтов, DDoS-атаки, несанкционированное использование API и др.;
- Анализирует действия пользователя, которые будут отсутствовать или отличаться от человеческих в случае бот-активности (прямолинейность траектории мышки, набор символов на клавиатуре, клики и т.д.);
- Выявляет использование средств автоматизации пользовательских действий;
- Проверяет IP-адреса и подсети, из которых приходят запросы к защищаемому ресурсу, на легитимность;
- Предоставляет дополнительные вердикты и скоринговые оценки в систему противодействия мошенничества Заказчика в целях снижения уровня ложноположительных выявлений мошенничества;
- Защищает параметры реальной пользовательской сессии от повторного использования ботами;

– Позволяет проводить анализ запросов с применением механизма гибкой настройки ограничителя запросов (за счет конфигурации параметров limiters и counters);

– Управляет входящими запросами при помощи капчи (антибот тестирование).

– Позволяет формировать пользовательские политики правил для выявления и блокировки ботов с использованием конструктора в пользовательском интерфейсе.

2 ТРЕБОВАНИЯ К СИСТЕМЕ

ПО функционирует в программно-аппаратных средах, отвечающих хотя бы одному из следующих требований:

- Среда поддерживается компилятором языка программирования Golang. Этому требованию соответствуют операционные системы на платформах Linux, Windows и macOS;
- Среда позволяет запустить систему контейнеризации Docker. ПО может функционировать в среде с ядром, поддерживающим контрольные группы и изоляцию пространств имён (namespaces); существуют сборки для Windows, MacOS (Intel and Apple chipset), популярных дистрибутивов Linux и ARM.

2.1 Технические требования

Для усредненной нагрузки в 10 тыс. запросов/сек (до 200 Мб/сек) необходимо выделить два физических сервера. Минимальные ресурсы сервера:

- CPU 6 ядер, 3 Ггц;
- RAM 16 ГБ;
- SSD 100 ГБ.

Чтобы минимизировать время обработки запросов к приложению, Preventive Proxy нужно настроить для проверки запросов только на динамический контент, а запросы на статический контент перенаправить через прокси-сервер в инфраструктуре защищаемого приложения.

При установке в инфраструктуре заказчика, сервера для Preventive Proxy рекомендуется разместить в дата-центре, где находится инфраструктура защищаемого приложения, или в одной подсети с инфраструктурой защищаемого приложения. Это позволит обращаться к Preventive Proxy без преобразования сетевых адресов (NAT) и сократить задержки между запросом и ответом.

3 УСТАНОВКА ЭКЗЕМПЛЯРА ПО

Для внедрения ПО в инфраструктуру приложения понадобятся:

– схема взаимодействия подсистем в инфраструктуре приложения;
– необходимые доступы к подсистемам;
– информация о дата-центрах (локации);
– контактные данные ответственных сотрудников.

В зависимости от способа встраивания (SaaS или On-premise) список запрашиваемых данных может отличаться.

На основе полученной информации специалисты Разработчика смогут предоставить рекомендации по внедрению и настройке ПО, а также скоординировать внедрение и запуск ПО. Эти данные можно передать специалистам Разработчика в любом удобном формате.

3.1 Схема установки ПО On-premise

Обработка входящего трафика в приложении работает следующим образом:

1. Весь трафик от фронтенда приходит на веб-сервер (рекомендуется использовать nginx);
2. Веб-сервер расшифровывает и отправляет трафик на бэкенд: сервера, скрипты, базы данных.

Классическая схема внедрения Preventive Proxy предполагает его установку на точку обработки трафика (на веб-сервер) в инфраструктуре Заказчика. Со стороны Заказчика сотрудник с правами администратора сможет настраивать, перезапускать и при необходимости отключать Preventive Proxy.

Такая схема установки Preventive Proxy называется установкой «в петлю» работает следующим образом:

1. Весь трафик от фронтенда идет на веб-сервер (чаще всего – nginx);
2. Веб-сервер отправляет трафик в Preventive Proxy, который проверяет и размечает трафик;
3. От Preventive Proxy размеченный трафик идет обратно на веб-сервер;
4. Веб-сервер блокирует бот-запросы (при работе в режиме блокировки), а легитимные запросы пользователей идут на бэкенд мобильного или веб-приложения: сервера, скрипты, базы данных.

3.2 Состав ПО

ПО состоит из основного модуля Preventive Proxy. Модуль отвечает за обработку клиентских запросов и выносит вердикт о наличии вредоносной бот-активности в режиме реального времени. Модуль поставляется в виде бинарного исполняемого файла для целевой АС.

Стандартный вариант поставки модуля Preventive Proxy — *.zip-архив, состоящий из файлов:

- proxy-core — бинарный исполняемый файл с основным модулем Preventive Proxy;
- config.yaml — конфигурационный файл для proxy-core;
- start.sh — скрипт для запуска proxy-core;
- README.md — файл с инструкциями для установки и запуска.

Дополнительно для работы ПО требуется встраивание ПО «F6 Fraud Protection», состоящего из двух модулей:

1. WebSnippet — клиентский модуль «F6 Fraud Protection» для защиты веб-ресурсов, реализован на языке JavaScript. Модуль загружается совместно со страницами защищаемого веб-ресурса.
2. Mobile SDK — клиентский модуль «F6 Fraud Protection» для защиты мобильных приложений, реализованные на языках Java и Objective-C/Swift. Модуль запускается совместно с мобильным приложением.

ПО «F6 Fraud Protection» производит сбор контрольных данных со страницы защищаемого приложения и устройства клиента и отсылает их для дальнейшего анализа в автоматизированную систему, пользовательский интерфейс которой доступен по ссылке https://fp.facct.ru. В целях обеспечения информационной безопасности, помимо использования протокола HTTPS при обращении к пользовательскому интерфейсу, используется ограничение на публичные IP-адреса/подсети, с которых это взаимодействие возможно. Для получения доступа к интерфейсу системы необходимо сообщить используемые IP-адреса/подсети, а также уточнить почтовый адрес для передачи тестовых учетных записей.

3.3 Действия по установке Preventive Proxy

1. Скачать тестовый образ ПО по ссылке: https://fp-demo.facct.ru/preventiveproxy/data.zip. ПО уже встроено на тестовом ресурсе https://fp-demo.facct.ru;
2. Скачать тестовые образы ПО «F6 Fraud Protection» по следующим ссылкам:

a. WebSnippet: https://fp-demo.facct.ru/js/fp.js

Данный модуль уже встроен на тестовом ресурсе: https://fp-demo.facct.ru;

b. Mobile SDK для Android OS: https://fp-demo.facct.ru/android/fp.apk;

c. Mobile SDK для iOS: https://fp-demo.facct.ru/ios/fp.ipa;

3. Добавить модули ПО «F6 Fraud Protection» в защищаемое приложение. Инструкция по установке и эксплуатации ПО «F6 Fraud Protection» предоставляется по запросу Заказчика.

4. Разместить исполняемый файл Preventive Proxy на прокси-сервере защищаемого приложения. В качестве прокси-сервера рекомендуется использовать NGINX.

5. Настроить конфигурацию модуля **auth_request NGINX**.

Пример конфигурации:

```
server {
  location = /auth {
    internal;
    proxy_connect_timeout 3s;
    proxy_send_timeout 15s;
    proxy_read_timeout 30s;
    proxy_pass https://<FP Backend URL:port>/auth;
    proxy_pass_request_body off;
    proxy_set_header Content-Length "";
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Original-Uri $request_uri;
    proxy_set_header X-Original-Host $server_name;
    proxy_set_header X-Request-Method $request_method;
    }
   ...
 }
```

6. Запустите исполняемый файл **proxy-core** командой:

```
./proxy-core -cfg config.yaml
```

В случае возникновения проблем следует обратиться по телефону +7 495 984-33-64 или по электронной почте - info@f6.ru.

4 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО

На Рисунке 1 изображены общие принципы функционирования ПО.

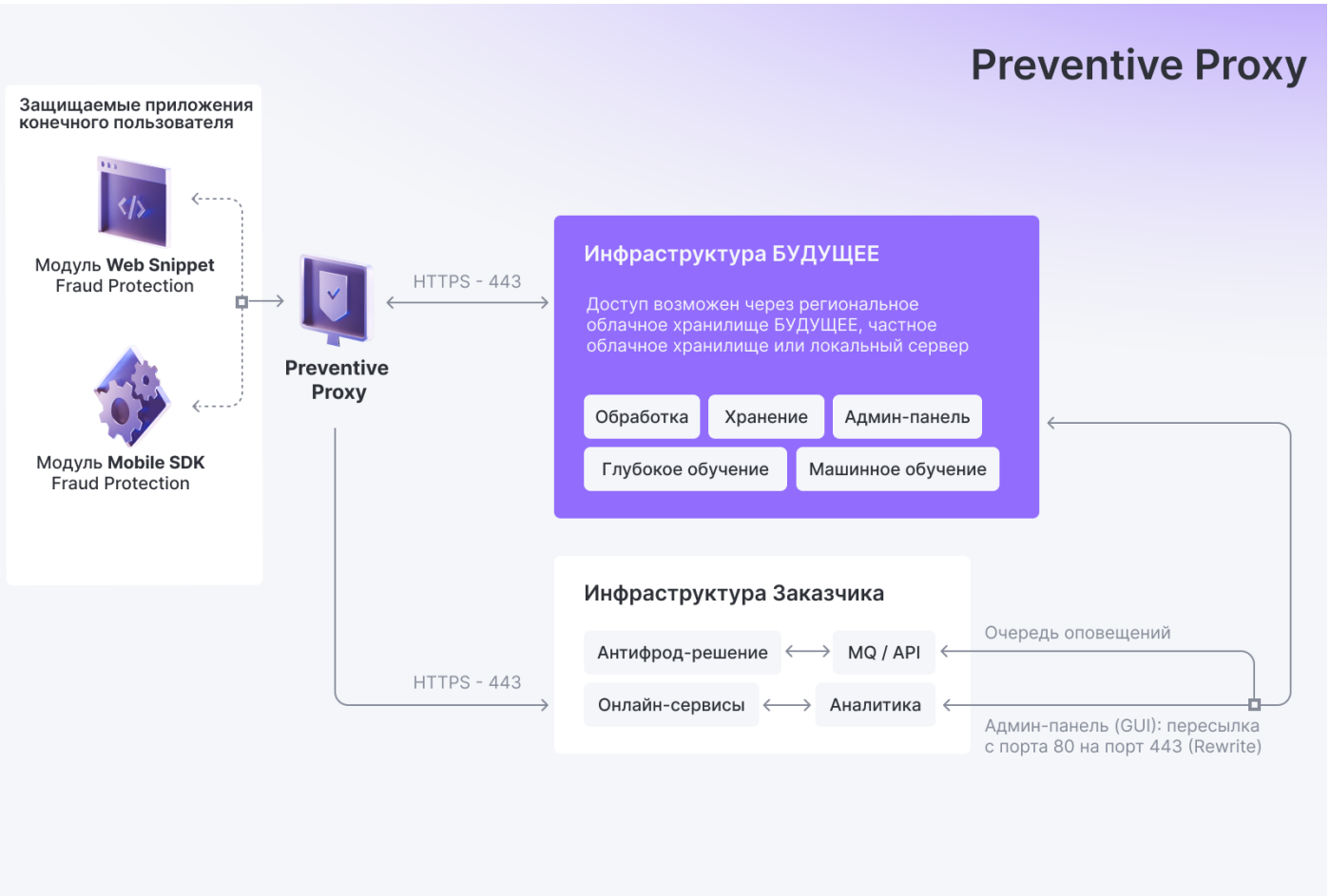

Рисунок 1. Общие принципы функционирования ПО.

Для работы Preventive Proxy понадобятся:

– клиентский модуль ПО «F6 Fraud Protection» (Web Snippet или Mobile SDK), который получает и передает в серверную часть поведенческие характеристики пользователя и окружения, в котором работает приложение;

– серверная часть ПО «F6 Fraud Protection» (Processing Hub). В ответ на данные, полученные из клиентского модуля, Processing Hub формирует и передает новый серверный файл cookie с вердиктом о наличии или отсутствии признаков бот-активности. При запросе из приложения клиентский модуль дополнительно формирует и передает клиентский файл cookie на базе серверного.

На основе данных, полученных из клиентского и серверного модулей «F6 Fraud Protection», Preventive Proxy проверяет наличие, корректность и уникальность файлов cookie на запросах с устройства пользователя, и на их основе принимает решение о наличии или отсутствии бот-активности в текущей пользовательской сессии.

5 ОБЯЗАННОСТИ И ФУНКЦИИ АДМИНИСТРАТОРА ЗАКАЗЧИКА

В обязанности администратора входит следующее:

- Произвести встраивание ПО в защищаемый веб-ресурс;
- Произвести встраивание ПО в защищаемое мобильное приложение;
- Поддерживать функционирование ПО;
- Установить и настроить обновленную версию ПО при получении экземпляра ПО с обновлением.

6 ОБРАБОТКА ТРАФИКА

Обрабатывать входящий трафик можно через:

– проксирование запросов через Preventive Proxy;
– разметку запросов с помощью auth-request в nginx.

Существует два основных вида запросов: на динамический и на статический контент. Обрабатывать запросы на статический контент через Preventive Proxy не эффективно. Такие запросы можно обрабатывать напрямую через веб-сервер, а динамические запросы, которые загружают серверную часть приложения, фильтровать через Preventive Proxy.

После установки модуля Preventive Proxy необходимо выбрать схему обработки запросов и настроить выбранный прокси-модуль (Preventive Proxy или nginx). Специалисты Разработчика могут предоставить примерный файл конфигурации, который будет адаптирован к инфраструктуре Заказчика.

6.1 Проксирование запросов через Preventive Proxy

Для работы модуля Preventive Proxy нужны два файла конфигурации - статический и динамический.

В статическом файле конфигурации указываются параметры запуска и работы Preventive Proxy. Этот файл конфигурации формируется специалистами Разработчика с учетом особенностей инфраструктуры заказчика и предпочтений по обработке трафика. Статический файл конфигурации обычно хранится в одной локации с файлом модуля Preventive Proxy и инициируется командой:

```
./proxy-core -cfg config.yaml
```

В динамическом файле конфигурации указываются правила загрузки и обработки трафика. На основе этих правил Preventive Proxy анализирует запросы пользователей мобильного или веб-приложения, обрабатывает значения токенов и принимает решения о наличии бот-активности. По умолчанию, динамический файл конфигурации хранится на сервере и формируется из настроек в панели администратора «F6 Fraud Protection». При необходимости он может быть предоставлен в виде *.yaml файла и загружен модулем Preventive Proxy в локальное хранилище.

6.2 Проксирование запросов с использованием модуля auth_request в nginx

Через модуль auth_request в nginx можно настроить обработку трафика для режима маркировки. Для этого нужна версия nginx не ниже 1.5.4.

При реализации такой схемы обработки трафика можно настроить для каких пользовательских запросов nginx запрашивает вердикт у «F6 Fraud Protection». Например, можно отфильтровывать запросы на выдачу статического контента или запросы из доверенных учетных записей для оптимизации загрузки Preventive Proxy. В зависимости от полученного вердикта nginx пропускает запрос на бэкенд инфраструктуры Заказчика или помечает его как бот-активность.

Для пользовательских запросов можно настроить:

- таймауты - если проверка запроса занимает больше времени, чем обычно, он будет перенаправлен в обход модуля Preventive Proxy;
- фильтр передаваемой информации - например, для отсеивания запросов на передачу выбранных типов файлов (запросов на статический контент);
- фэйловер - механизм перенаправления запросов, например, когда заданное число запросов не дошло до Preventive Proxy, отправка запросов переключится на запасную ноду или пойдет в обход Preventive Proxy.

В работе модуля auth_request понадобится использовать заголовки:

- X-Real-IP - для передачи исходного (начального) IP-адреса запроса;
- X-Original-Uri - для передачи URI исходной точки запроса;
- X-Original-Host - для передачи адреса исходного сервера, обрабатывающего запрос;
- X-Request-Method - для передачи HTTP-метода запроса.

Файл конфигурации формируется специалистами Разработчика с учетом особенностей инфраструктуры Заказчика и предпочтений по обработке трафика.

6.3 Правила обработки трафика

Preventive Proxy проверяет трафик, поступающий к мобильному или веб-приложению Заказчика согласно правилам, которые настраиваются в разделе «Боты» ПО «F6 Fraud Protection» на вкладке «Настройки». На основе этих правил Preventive Proxy анализирует запросы пользователей, обрабатывает значения токенов и принимает решения о наличии бот-активности.

Во время обработки трафика Preventive Proxy добавляет к пользовательским запросам служебные заголовки, содержащие дополнительную информацию и вердикт о наличии или отсутствии вредоносной бот-активности.

6.3.1 Обработка трафика

Для каждого правила обработки трафика можно задать действие, которое будет выполняться, если это правило сработает. Preventive Proxy может выполнять следующие действия с пользовательскими запросами:

- блокировать (block) — Preventive Proxy блокирует все пользовательские запросы, подпадающие под действие правила;
- защищать (protect) — Preventive Proxy блокирует только запросы с признаками подозрительной активности;
- замедлять (shape) — Preventive Proxy замедляет поток запросов с признаками подозрительной активности, ограничивая их количество в минуту;
- помечать (mark) — Preventive Proxy помечает запросы с признаками подозрительной активности, но не блокирует их;
- пропускать (pass) — Preventive Proxy пропускает весь входящий трафик.

С помощью комбинации правил можно гибко настраивать проверку входящего трафика для различных ситуаций и политик безопасности.

6.3.2 Настройка правил

Чтобы наиболее полно и эффективно обрабатывать входящий трафик, можно задать неограниченное количество правил.

Для каждого правила необходимо указать приоритет относительно других активных правил и действие, которое выполняется, если пользовательский запрос активирует это правило. Настройки правил хранятся в динамическом файле конфигурации, их можно менять через панель администратора «F6 Fraud Protection» в разделе «Боты».

6.3.3 Правило по умолчанию

Правило по умолчанию — правило с самым низким приоритетом, находится внизу списка на вкладке «Настройки». Если не сработало ни одно правило из списка активных правил, к пользовательскому запросу будет применяться правило по умолчанию.

Правило по умолчанию необходимо задать во время первичной настройки Preventive Proxy. Во время настройки правила по умолчанию можно выбрать действия:

- защищать (protect) — блокировать только запросы с признаками подозрительной активности;
- помечать (mark) — помечать запросы с признаками подозрительной активности, но не блокировать их;

– пропускать (pass) — пропускать весь входящий трафик.

Правило по умолчанию не может выполнять действие «блокировать», потому что в этом случае все запросы, которые не попали под действие других правил, будут заблокированы.

7 ПОДДЕРЖАНИЕ ФУНКЦИОНИРОВАНИЯ ПО

Поддержание функционирования ПО заключается в контроле настроек, проведенных в рамках установки ПО. Иных регламентных мероприятий со стороны Заказчика ПО не требует.