Гарда БД

Функциональная спецификация

Модуль "Агент контроля подключений"

Дата выпуска:	22.06.2022
Статус документа:	Released
Версия ПО:	4.19.1

Содержание

1. Введение

1.1. Аннотация

Данный документ представляет собой Функциональную спецификацию к программному модулю «Агент контроля подключений», входящий в состав программного обеспечения «Гарда БД».

1.2. О компании

«Гарда Технологии» – российский разработчик систем защиты от внутренних и внешних угроз информационной безопасности, противодействия мошенничеству и расследования инцидентов.

Решения «Гарда Технологии» занимают лидирующие позиции на российских рынках решений информационной безопасности:

- защиты от DDoS-атак операторского класса.
- защиты баз данных.
- фрод-мониторинга порядка пропуска трафика операторов связи.
- DLP-систем.

Разработки аппаратно-программных решений информационной безопасности ведутся с 2005 года. Исследовательский центр компании обладает 5 патентами на уникальные технологии. Решения «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, операторах связи и государственных структурах России и СНГ. Подробнее – на gardatech.ru

1.3. Техническая поддержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании "Гарда Технологии":

- Тел. +7 (831) 422-12-20 (с 9-00 до 18-00 по Московскому времени).
- Email: gbd.support@gardatech.ru.

2. Функциональные возможности

2.1. Поддерживаемые способы перехвата

2.1.1. Описание

Агент поддерживает три способа перехвата в зависимости от используемого типа соединения:

- *external TCP* — соединения по протоколу IPv4/TCP с удалённых хостов.
- *loopback TCP* — соединения по протоколу IPv4/TCP с локального хоста. Соединения проходят через виртуальный loopback-интерфейс системы. Это как соединения с приёмником/источником из подсети 127.0.0.0/8, так и соединения, в которых адрес приёмника равен адресу источника и совпадает с адресом, назначенным внешнему сетевому интерфейсу.
- *локальный* — соединения внутри одного хоста, не являющиеся loopback TCP:
  - соединения по UNIX-сокетам;
  - соединения по именованным каналам в Windows;
  - соединения по пайпам.

При перехвате локального трафика, а также перехвате loopback/external TCP не через *pcap* захватываются только полные сессии. Если перехват запущен после инициации сессии (*accept* сокета или открытие пайпа/именованного канала), то сессия не будет перехвачена даже частично. При перехвате TCP через *pcap* возможен разбор уже начатой сессии, если на сниффере включена *tcp recovery* для соответствующего протокола.

Поддерживается указание нескольких анализаторов для отправки данных. В случае проблем соединения с основным анализатором агент переключится на резервный. Отправляться данные на резервный анализатор будут до тех пор, пока с ним не разорвётся связь, после чего агент переключится на основной анализатор.

Агент не сохраняет накопленные в буферах данные при перезапуске сервиса агента, при остановке перехвата.

Агент позволяет динамическую перенастройку перехвата во время работы. При этом:

- Если в новых настройках требуется новый перехватчик, он будет запущен.
- Если в новых настройках какой-либо перехватчик не требуется, он будет остановлен.
- Если перенастройка не коснулась какого-либо перехватчика, то его состояние не изменится.
- Перехватчик, чья настройка изменилась, будет перезапущен. Это может привести к пропуску перехвата данных и/или потере сессий, открытых до перезапуска перехватчика.

Ограничения:

- отсутствует пересылка данных при проблемах соединения с анализатором.

2.1.2. Настройки

Настройка способов перехвата ведётся через конфиг-файл *dbs_agent.cfg*.

Параметр *EXTERNAL_INTERCEPTION_METHOD* задаёт способ перехвата внешнего TCP-трафика, если такой метод поддерживается платформой:

- **pcap** — через библиотеку захвата пакетов pcap;
- **module** — через драйвер;
- **dtrace** - через скрипт DTrace.

Параметр *LOOPBACK_INTERCEPTION_METHOD* задаёт способ перехвата loopback TCP-трафика, если такой метод поддерживается платформой:

- **pcap** — через библиотеку захвата пакетов pcap;
- **module** — через драйвер;
- **dtrace** - через скрипт DTrace.

Параметр *KERNEL_MODULE* выбирает способ перехвата локального трафика:

- **true** — через модуль ядра Linux / драйвер в Windows / расширение ядра в AIX;
- **false** — в пространстве пользователя.

2.1.3. Перехват через pcap

Может применяться для перехвата:

- external TCP;
- loopback TCP.

Поддерживается на всех платформах.

Не поддерживает блокировку соединений. Игнорирование соединений возможно только для правил, состоящих из критериев по IP-адресу источника и только по нему.

Позволяет перехватывать *исходящий* трафик, т.е. соединения на удалённый хост, инициированные с машины, на которой установлен агент.

Поддерживается перехват VLAN-трафика (802.1q). Включается параметром *capture_vlan*.

Максимальная длина перехватываемого пакета — 1 Мб. Пакет длиннее 64 килобайт может возникнуть при включенном режиме *TCP Segmentation Offload* в драйвере сетевой карты, также известном как *Large Send Offload (LSO)* и *Large Receive Offload (LRO)*.

Перехваченные данные TCP loopback изменяются следующим образом: в заголовках IP и TCP вместо IP-адреса и порт сервера заменяются на первый из IP-адресов и портов поставленной на перехват базы данных. Если на перехват поставлено несколько баз данных и/или, то выбирается наиболее подходящая из них (по порту). Если порт не найден, то выбирается первая попавшаяся база данных.

2.1.4. Перехват через модуль ядра/драйвер

Может применяться для перехвата:

- external TCP;
- loopback TCP;
- локальных соединений.

Выбранные интерфейсы для перехвата внешнего TCP-трафика игнорируются. Трафик выбирается по сочетанию IP:port, указанному в настройках базы данных. При открытии локальной/loopback TCP сессии агент дополнительно отправляет на анализатор имя пользователя ОС, который открыл сессию. При включенной настройке DETECT_LOGIN_SESSION дополнительно отправляется имя, под которым пользователь зашел в систему (например, через SSH).

Ограничения:

- В случае перехвата loopback TCP на Windows и Oracle BEQ на UNIX системах агент может не успевать определять имя пользователя ОС для коротких сессий (< 1 сек).
- В случае обращения к базе посредством screen, cron или другим подобным методом, агент не сможет корректно определить логин пользователя.

2.1.5. Перехват через DTrace

Может применяться для перехвата:

- external TCP;
- loopback TCP;
- локальных соединений.

Выбранные интерфейсы для перехвата внешнего TCP-трафика игнорируются. Трафик выбирается по сочетанию IP:port, указанному в настройках базы данных. При открытии локальной/loopback TCP сессии агент дополнительно отправляет на анализатор имя пользователя ОС, который открыл сессию. При включенной настройке DETECT_LOGIN_SESSION дополнительно отправляется имя, под которым пользователь зашел в систему (например, через SSH). Если запрос к базе выполняется в зоне, к которой подключились через zlogin, то агент в качестве логина отправит имя пользователя, с которым вызван zlogin (опция "-l", по умолчанию root).

2.1.6. Перехват через ptrace

Работает на Linux в пространстве пользователя. Может применяться для перехвата локальных соединений. При открытии локальной сессии агент дополнительно отправляет на анализатор имя пользователя ОС, который открыл сессию.