ГАРДА
ТЕХНОЛОГИИ

ООО "Гарда Технологии"

Руководство администратора

ПК "Периметр"

Нижний Новгород, 2022

Оглавление

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство администратора к программному модулю «Анализатор», входящий в состав программного обеспечения ПРОГРАММНЫЙ КОМПЛЕКС «ПЕРИМЕТР».

1.2 Термины, определения и сокращения

Термин	Значение
ПК	ПРОГРАММНЫЙ КОМПЛЕКС «ПЕРИМЕТР»
Система	ПК «ПЕРИМЕТР»
Модуль	Модуль «Анализатор»
СПД	Сеть передачи данных
БРП	База решающих правил
DoS	Сетевая (компьютерная) атака, направленная на отказ в обслуживании
DDoS	DoS-атака, выполняемая одновременно с большого числа компьютеров

1.3 Использование имен, номеров телефонов, сетевых адресов

Все регистрационные имена пользователей, а также номера телефонов, имена и другие данные абонентов, используемые в Руководстве, являются вымышленными, а IP-адреса не соответствуют их действительным владельцам. Любые совпадения случайны.

1.4 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.

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

1.5 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: ddos.support@gardatech.ru

2 Назначение Системы

ПРОГРАММНЫЙ КОМПЛЕКС «ПЕРИМЕТР» (далее ПК «ПЕРИМЕТР») представляет собой систему обнаружения и противодействия сетевым атакам типа «Отказ в обслуживании DoS/DDoS» (далее DDoS) и анализа трафика на сети передачи данных (далее СПД).

Решение данной задачи основано на:

- постоянном контроле состояния трафика СПД и его многостороннем анализе;
- обнаружении отклонений параметров трафика (аномалий);
- интеллектуальной фильтрации трафика с блокированием вредоносной составляющей и пропуском легитимной.

Модуль Анализатор является средством мониторинга трафика СПД и выявления аномалий, которое осуществляет непрерывный анализ трафика контролируемой сети и при обнаружении атаки выдает команды маршрутизирующему оборудованию на первичную очистку и последующее перенаправление трафика на Очиститель.

В зависимости от поставленных задач, Анализатор может быть реализован автономно, либо вместе с Очистителем в рамках одного аппаратного модуля.

3 Установка модуля «Анализатор»

3.1 Развертывание комплекса

В рамках развертывания комплекса необходимо произвести приемку согласно комплектности поставки и проверку информации, записанной на оптический диск установочного комплекта.

Для функционирования ПК «Периметр» необходимо установить операционную систему Debian 10.0. Дистрибутив доступен на официальном сайте (https://cdimage.debian.org/cdimage/archive/10.7.0/amd64/iso-cd/). Поддерживаемая архитектура - amd64, поддерживаемая версия ядра системы - 4.19.0-6-amd64.

Действия по формированию функциональной среды требуют наличие прав суперпользователя.

После разметки дискового пространства и установки необходимых для функционирования используемой аппаратной платформы драйверов и утилит, выполняется установка модуля «Анализатор» с помощью менеджера пакетов:

```
apt-get install --assume-yes --allow-unauthenticated synta -o DPkg::Options::="--force-
↪overwrite"
```

3.1.1 Включение модуля «Анализатор»

Модуль Анализатор подключается через следующие логические интерфейсы:

- интерфейс подключения к технологической сети - предоставляющий возможность взаимодействия с модулями Лидер и Очиститель;
- интерфейс взаимодействия с маршрутизирующим оборудованием - данный интерфейс предназначен для получения модулем данных, передаваемых по протоколам NetFlow, SNMP, а также для взаимодействия в рамках устанавливаемых BGP-сессий;
- интерфейс горячего резерва - данный интерфейс применяется для обмена информацией с резервным модулем Анализатор, в случае применения режима горячего резерва.

Общий принцип подключения комплекса в режиме BGP-ответвления представлен на рисунке 1.

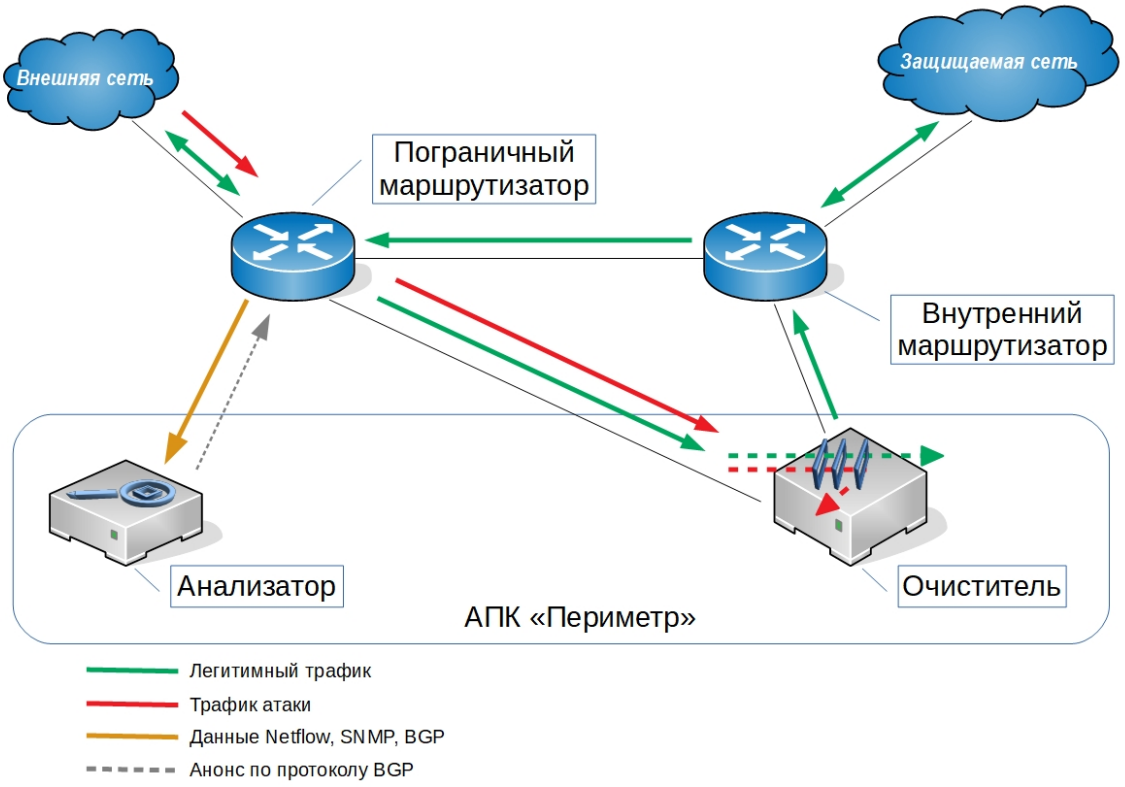

Рис. 1 Общий принцип подключения модуля «Анализатор».

4 Настройка модуля «Анализатор»

В случае автономной реализации (без модуля Лидер) настройка параметров модуля осуществляются напрямую через Модуль «Анализатор».

4.1 Настройка границы сети

Необходимо произвести:

- настройку взаимодействия комплекса со всеми пограничными маршрутизаторами по протоколам Netflow, SNMP, BGP. Если будут настроены не все маршрутизаторы, то трафик будет учтен не полностью и аномальное поведение трафика на этих устройствах не будет выявляться;
- настройку адресного пространства контролируемой СПД - данная информация позволяет по полученной информации определить принадлежность трафика контролируемой сети;
- классификацию интерфейсов пограничных маршрутизаторов. Данная настройка, совместно с настройкой адресного пространства, позволяет однозначно определять принадлежность трафика контролируемой СПД и его направление (входящий, исходящий, транзитный). В рамках классификации комплекс позволяет настраивать следующие типы интерфейсов:
  - внешний – интерфейс, направленный в сторону соседней сети;
  - внутренний – интерфейс, направленный в контролируемую сеть;
  - магистральный - интерфейс, трафик через который направлен как внутрь контролируемой СПД, так и вне её;
  - смешанный – интерфейс, трафик которого может быть как внешним, так и внутренним;
  - игнорируемый - интерфейс, трафик через который анализатор не учитывает независимо от того, является ли этот трафик исходящим или входящим.

4.2 Настройка под сетевую инфраструктуру

Все необходимые настройки комплекса для взаимодействия с сетевой инфраструктурой (маршрутизаторами СПД) выполняются в разделе меню «Администрирование / Мониторинг / Инфраструктура». Доступно конфигурирование следующих объектов сетевой инфраструктуры:

- групп маршрутизаторов;
- маршрутизаторов;
- интерфейсов.

4.3 Настройка контролируемой сети

Чтобы настроить описание контролируемой СПД:

1. Перейдите на страницу мониторинга сети «Администрирование / Мониторинг / Сеть»;
2. Перейдите на вкладку «Описание»;
3. Заполните следующие поля:
   - Название - название контролируемой СПД;
   - Номера магистральных AS - ASN магистральных автономных систем, принадлежащих контролируемой СПД;
4. Нажмите кнопку «Сохранить» или, для отмены внесённых изменений, нажмите кнопку «Отмена».

4.4 Настройка Маршрутизаторов

Маршрутизаторы являются основными устройствами, с которыми модуль «Анализатор» взаимодействует в рамках выполнения задач. Все действия по настройке маршрутизаторов выполняются на экране интерфейса «Администрирование / Мониторинг / Инфраструктура / Маршрутизаторы».

4.5 Настройка NetFlow

Данные, полученные по протоколу NetFlow, служат для анализа трафика. При соответствующих настройках эти данные поступают как с маршрутизаторов, так и с сенсоров контролируемой СПД.

Чтобы настроить параметры получения данных по протоколу NetFlow необходимо:

1. перейти на вкладку NetFlow;
2. установить параметр «Поддержка NetFlow», который активирует взаимодействие с данным маршрутизатором по протоколу NetFlow;
3. ввести IP-адрес маршрутизатора в поле IP-адрес источника NetFlow;
4. выбрать один из пунктов раскрывающегося списка «Получать данные»:
   - PCAP - вариант, если IP-адрес анализатора не указан как получатель данных по протоколу NetFlow на маршрутизаторе (трафик перенаправляется на анализатор средствами СПД);
   - Сокет - вариант, если IP-адрес анализатора указан как получатель данных по протоколу NetFlow на маршрутизаторе;
5. заполнить следующие поля:
   - локальный порт - номер локального порта, на который маршрутизатор отправляет NetFlow (обязательное поле в режиме Сокет);

- Sampling rate - частота выборки по заголовку NetFlow-датаграмм (для автоматического определения значения по NetFlow, оставьте поле пустым или введите значение «0»);

6. для включения функции масштабирования на основе SNMP, необходимо установить параметр «SNMP-scaling»;
7. чтобы анализатор автоматически отправлял уведомление об отсутствии данных по протоколу NetFlow, установить параметр «Предупреждение об отсутствии потока»;
8. при необходимости можно выбрать интерфейсы, данные netflow с которых будут учитываться при анализе (переход к выбору осуществляется нажатием на кнопку «Выбрать интерфейсы для мониторинга»);
9. если установлен флажок «Предупреждение об отсутствии потока», задать время ожидания NetFlow-датаграмм в поле «Время ожидания NetFlow перед генерацией уведомления». В случае превышения заданного значения анализатор выявляет аномалию;
10. при необходимости установить параметр «Проверка на поддельный источник NetFlow (по TTL)», при установленном параметре, в случае обнаружения поддельного NetFlow, система создаст аномалию;
11. при необходимости отправки принимаемого потока netflow на другие коллекторы, укажите их IP адреса и порты, на которые необходимо осуществлять пересылку в поле «Список адресов для пересылки NetFlow».

4.6 Настройка BGP

Протокол динамической маршрутизации используется комплексом для перенаправления трафика на очистку, составления отчетов и сопоставления трафика с наблюдаемыми объектами, заданным критериями по BGP-атрибутам.

Чтобы настроить соединение анализатора с маршрутизатором по протоколу BGP необходимо:

1. перейти на вкладку BGP;
2. установить параметр «Поддержка BGP», который активирует взаимодействие с данным маршрутизатором по протоколу BGP;
3. при необходимости в поле «Использовать таблицу маршрутизации с:» выбрать маршрутизатор, таблица маршрутизации которого будет использоваться при сопоставлении данных Netflow, полученных с редактируемого маршрутизатора. В случае выбора данного параметра, по умолчанию будут недоступны параметры настройки BGP-сессии, используемой для перенаправления трафика. Если данная сессия необходима, установите параметр «Задать параметры для подключения к устройству по BGP для анонсирования маршрутов»;
4. заполнить следующие поля:
   - IP BGP-соединения - IP-адрес маршрутизатора, для установки BGP-сессии;
   - номер удаленной BGP AS - ASN маршрутизатора;
   - номер локальной AS - ASN анализатора;
   - MD5 секрет;

- IP-адрес Blackhole-фильтрации - необязательный параметр, задающий адрес blackhole маршрута для данного маршрутизатора;
- сообщества - необязательный параметр, устанавливающий BGP-community для анонсов. На данном экране присутствуют предустановленные BGP-community (LOCAL_AS, NO_ADVERTISE, NO_EXPORT, NO_PEER);

5. Чтобы анализатор установил соединение и получал таблицы маршрутизации, необходимо установить параметр «Разрешить установку пиринговых отношений между маршрутизатором и анализатором».

4.7 Настройка SNMP

Данные, полученные по протоколу SNMP, содержат статистику трафика, проходящего через интерфейсы, статистику работы маршрутизатора, а также названия и описания интерфейсов. При использовании сабинтерфейсов, существует возможность копирования описания из базового интерфейс в сабинтерфейс, если он единственный.

Чтобы настроить соединение анализатора с маршрутизатором по протоколу SNMP необходимо:

1. перейти на вкладку SNMP.
2. выбрать один из пунктов раскрывающегося списка «Версия SNMP»;
3. для версии 2c заполнить следующие поля:
   - Query IP - IP-адрес маршрутизатора, для работы по протоколу SNMP;
   - Сообщества - используемое SNMP сообщество;
4. для версии 3 выбрать один из пунктов раскрывающихся списков «Безопасность» и «Протокол аутентификации», а также заполнить следующие поля:
   - Query IP - IP-адрес маршрутизатора, для работы по протоколу SNMP;
   - пользователь;
   - безопасность - тип аутентификации;
   - протокол аутентификации - используемый протокол (для типов аутентификации authNoPriv и authPriv);
   - пароль аутентификации (для типов аутентификации authNoPriv и authPriv);
   - приватный ключ (для типа аутентификации authPriv);
   - контекст (для типов аутентификации authNoPriv и authPriv);
5. при необходимости установить параметр «Обрабатывать только интерфейсы с NetFlow». Установка параметра ограничивает опрос маршрутизатора только теми интерфейсами, с которых приходит NetFlow, что позволяет существенно снизить нагрузку на маршрутизатор.

5 Обновление модуля «Анализатор»

Предприятие-разработчик на этапе сопровождения может осуществлять периодический выпуск обновлений.

Определены три типа обновлений Изделия:

- 1 тип – обновление баз данных, необходимые для поддержания актуальности БРП;
- 2 тип – обновление, направленное на устранение выявленных уязвимостей (критическое обновление) ПК;
- 3 тип – обновление, направленное на добавление и/или совершенствование реализации функций безопасности, на расширение числа поддерживаемых программных и аппаратных платформ (обновление версии ПК).

Информирование потребителей о выпуске обновлений Изделия 2 и 3 типа осуществляется путем рассылки информационных уведомлений потребителям Изделия.

Обновление модуля «Анализатор» осуществляется с помощью менеджера пакетов.