ГАРДА
ТЕХНОЛОГИИ

ООО "Гарда Технологии"

Руководство администратора

Модуль Лидер ПК "Периметр"

Нижний Новгород, 2022

Оглавление

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство пользователя к программному модулю «Лидер», 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 «Лидер»
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 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.

3 Установка модуля «Лидер»

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 «Лидер» с помощью менеджера пакетов:

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

3.1.1 Включение модуля «Лидер»

Модуль Лидер подключается через следующие логические интерфейсы:

- интерфейс управления - обеспечивающий возможность подключения пользователей к web-интерфейсу;
- интерфейс подключения к технологической сети - предоставляющий возможность взаимодействия модуля Лидер с модулями Анализатор;
- интерфейс горячего резерва - данный интерфейс применяется для обмена информацией с резервным модулем Лидер, в случае применения режима горячего резерва.

Все логические интерфейсы могут быть исполнены как в рамках одного физического интерфейса, так и нескольких.

4 Настройка модуля «Лидер»

Настройка Модуля включает несколько этапов:

- Настройка границы сети:
  - настройку взаимодействия комплекса со всеми пограничными маршрутизаторами по протоколам Netflow, SNMP, BGP;
  - настройку адресного пространства контролируемой СПД;
  - классификацию интерфейсов пограничных маршрутизаторов.
- Настройка под сетевую инфраструктуру
  - групп маршрутизаторов;
  - маршрутизаторов;
  - интерфейсов.
- Настройка контролируемой сети:
  - Название - название контролируемой СПД;
  - Номера магистральных AS - ASN магистральных автономных систем, принадлежащих контролируемой СПД.
- Настройка Маршрутизаторов
- Настройка NetFlow:
  - IP-адрес источника NetFlow;
  - Способ получения данных;
  - Локальный порт;
  - Частота выборки.
- Настройка BGP:
  - 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.
- Настройка SNMP:
  1. для версии 2c заполнить следующие поля:
     - Query IP - IP-адрес маршрутизатора, для работы по протоколу SNMP;
     - Сообщества - используемое SNMP сообщество;

2. 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);

Настройка модуля «Лидер» совпадает с настройкой модуля «Анализатор» и подробно описана в документе «Периметр. Руководство администратора. Анализатор»

5 Обновление модуля «Лидер»

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 «Лидер» осуществляется с помощью менеджера пакетов.