ГАРДА
ТЕХНОЛОГИИ

ООО "Гарда Технологии"

Функциональная спецификация

Модуль Хранилище ПК "Периметр"

Нижний Новгород, 2022

Оглавление

1 Введение

1.1 Аннотация

Данный документ представляет собой Функциональную спецификацию к программному модулю «Хранилище», 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 «Хранилище»
СПД	Сеть передачи данных
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.

Хранилище представляет собой аппаратно-программное средство хранения и обработки базы flow-записей.

В зависимости от объема нагрузки на комплекс, модуль Хранилище может поставляться в рамках одного аппаратного модуля, либо совместно с Анализатором.

3 Функциональные возможности

3.1 Функциональные возможности модуля «Хранилище»

Хранилище – подсистема хранения данных, которая осуществляет долговременное хранение детализированной информации о трафике СПД для оперативного построения отчетов с возможностью фильтрации и группировки по параметрам трафика.

База данных flow-записей предоставляет доступ к информации netflow, получаемой ПК «ПЕРИМЕТР». Flow-записи являются источником данных для аналитических отчетов и детекторов DDoS-атак. Flow-записи сопоставляются с данными полученными по протоколу BGP, а также с наблюдаемыми объектами, сконфигурированными администратором Системы.

Модуль Хранилище расчитан (параметры на один Модуль) на объем хранения данных не менее 1 месяца, число одновременно выполняемых запросов на получение данных - до 15.

Примечание. Ввиду значительного объема принимаемых Комплексом данных netflow, хранение flow-записей возможно только на специализированных внешних модулях хранения , позволяющих хранить и обрабатывать большой объём данных.

3.2 Функциональные возможности компонентов модуля «Хранилище»

- компонент осуществляющий интерфейс управления Модуля;
- компонент осуществляющий получение и обработку информации источников Netflow данных;
- компонент осуществляющий механизмы синхронизации.

3.3 Интерфейсы модуля «Хранилище»

Хранилище имеет интерфейсы взаимодействия с модулями Анализатор для управления и обмена данными базы flow-записей.

3.4 Аппаратная реализация

Модуль комплекса исполнен в виде серверного устройства, устанавливаемого в 19" серверные шкафы и стойки.

3.5 Программная реализация

Модуль «Хранилище» устанавливается в среде функционирования операционной системы Debian 10 или AltLinux 8SP.

4 Работа с Хранилищем

Настройка и управление работы модуля Хранилище производится из модуля Анализатор, либо (если установлен) из модуля Лидер.

Для работы с базой flow-записей необходимо перейти в меню «Отчёты / Сырой NetFlow / Хранилище». Экран разделен на три блока:

- фильтр и группировка – блок, выполняющий функцию конструктора запросов к базе данных flow-записей; поддерживается поиск по полям flow-записи, ASN источника и назначения, GeoIP источника и назначения, а также ассоциированным с этой записью наблюдаемым объектам и сигнатурам атак;
- графическое представление – временной ряд выбранного в блоке фильтра трафика в единицах объема трафика (bps) или количества пакетов (pps);
- табличное представление – блок аналитической информации в виде сетки данных, может содержать отдельные flow-записи или агрегированную информацию по трафику (набор полей flow-записей), сгруппированную по заданным в блоке фильтра критериям.

Информация, получаемая из хранилища flow-записей, может быть экспортирована в виде текстового файла в CSV-формате. Для этого необходимо перейти по ссылке «Скачать», расположенной над табличным представлением.