ГАРДА
ТЕХНОЛОГИИ

ООО "Гарда Технологии"

Руководство пользователя

Модуль Хранилище ПК "Периметр"

Нижний Новгород, 2022

Оглавление

1 ВВЕДЕНИЕ

1.1 Аннотация

Данный документ представляет собой Руководство пользователя 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»
Комплекс	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.

3 НАЧАЛО РАБОТЫ

Настройка и администрирование комплекса осуществляется через графический интерфейс пользователя (далее web-интерфейс) модуля Анализатор либо модуля Лидер (если он установлен).

Чтобы открыть web-интерфейс:

1. Запустите web-браузер.
2. Установите в настройках следующие параметры отображения страниц:
   - Использовать безопасное соединение;
   - Разрешить появление всплывающих окон;
   - Разрешить исполнение скриптов Javascript
   - Разрешить приём файлов cookie.
3. Введите в поле адресной строки web-браузера https://IP-address, где IP-address – это адрес интерфейса управления модуля Лидер (если комплекс не поставлялся с данным модулем, то необходимо указать адрес модуля Анализатор), настроенный в рамках подготовки комплекса к эксплуатации.
4. На странице Аутентификация пользователя введите имя учётной записи пользователя и пароль (при проверке введённых данных система учитывает регистр символов), которые были настроены в рамках подготовки комплекса к эксплуатации.
5. Нажмите кнопку Войти.

4 ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

4.1 База данных flow-записей

База данных flow-записей предоставляет доступ к информации netflow, получаемой Комплексом. 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 Комплекса.

4.2 Работа с модулем «Хранилище»

Для работы с базой flow-записей необходимо перейти в меню «Отчёты / Сырой NetFlow / Хранилище».

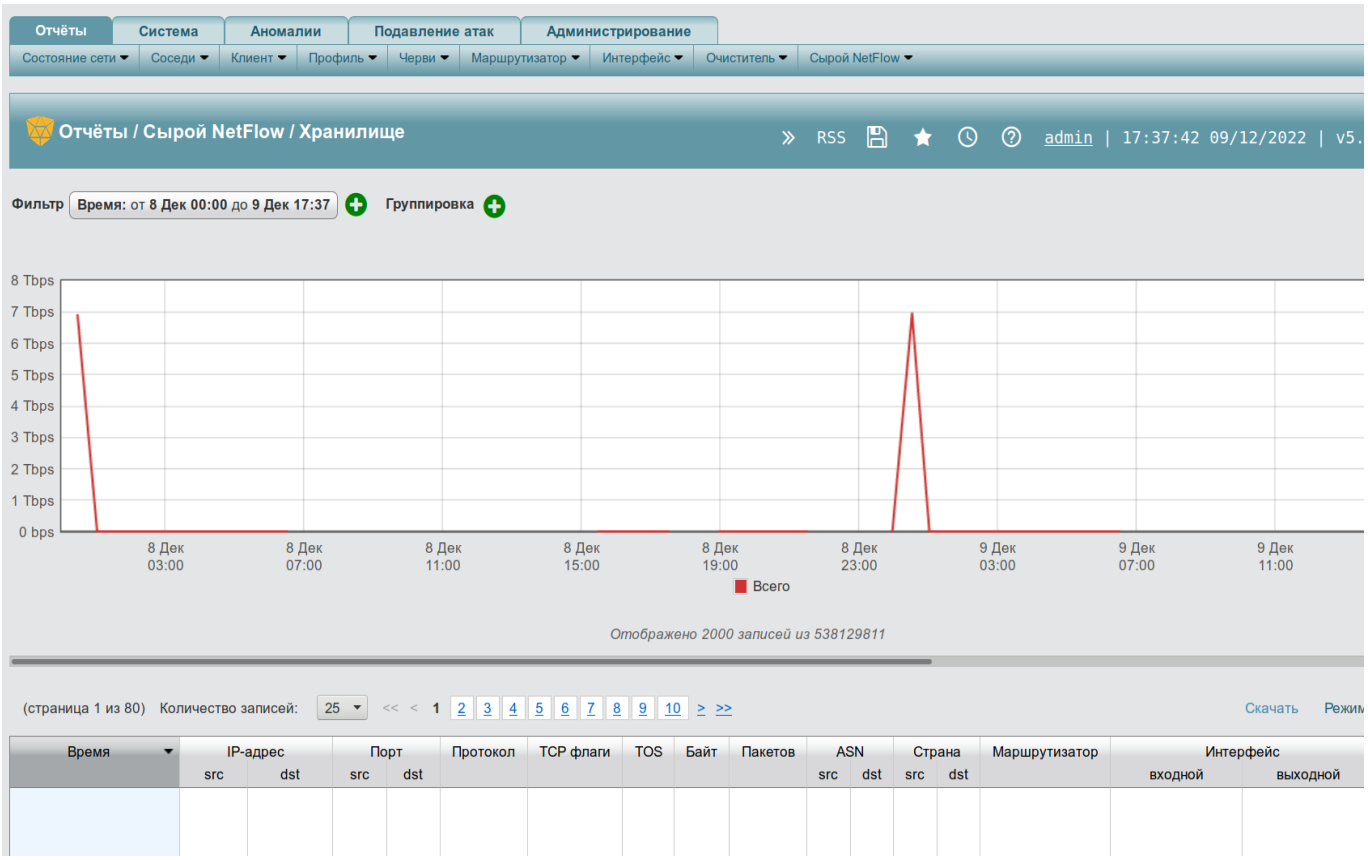

Рис. 1 Работа с Хранилищем.

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.

4.2.1 Табличное представление

В табличном представлении отображаются следующие данные:

- Время
- IP-адрес
  - src
  - dst
- Порт
  - src
  - dst
- Протокол
- TCP флаги
- TOS
- Байт
- Пакетов
- ASN
  - src
  - dst
- Страна
  - src
  - dst
- Маршрутизатор
- Интерфейс
  - входной
  - выходной
- Объекты
- DoS сигнатуры
- Время старта флоу
- Длительность, мс
- Причина экспорта

4.2.2 Фильтр

Фильтр позволяет выбрать следующие значения:

- IP-адрес
- IP-адрес src
- IP-адрес dst
- Порт
- Порт src
- Порт dst
- Протокол
- Протокол/порт
- TCP флаг
- ASN
- ASN src
- ASN dst
- Страна
- Страна src
- Страна dst
- Маршрутизатор
- Интерфейс
- Интерфейс входной
- Интерфейс входной 0
- Интерфейс выходной
- Интерфейс выходной 0
- Объект
- Граница объекта
- Версия IP
- Размер пакета
- DoS сигнатура

4.2.3 Группировка

Группировка позволяет выбрать следующие значения:

- IP-адрес
- IP-адрес src
- IP-адрес dst
- Порт
- Порт src
- Порт dst
- Протокол
- TCP флаг
- ASN
- ASN src
- ASN dst
- Страна
- Страна src
- Страна dst
- Маршрутизатор
- Интерфейс
- Интерфейс входной
- Интерфейс выходной
- Объект
- Версия IP
- DoS сигнатура

4.2.4 Экспорт

Информация, получаемая из хранилища flow-записей, может быть экспортирована в виде текстового файла в следующих форматах:

- CSV
- Excel

Для этого необходимо перейти по ссылке «Скачать», расположенной над табличным представлением.

5 ЗАВЕРШЕНИЕ РАБОТЫ

Для завершения работы с Комплексом необходимо:

- нажать кнопку «Выход» в правом верхнем углу страницы веб-интерфейса;
- закрыть веб-браузер.