ООО "Гарда Технологии"

Функциональная спецификация

Модуль Очиститель ПК "Периметр"

Нижний Новгород, 2022

Оглавление

1 Введение

1.1 Аннотация

Данный документ представляет собой Функциональную спецификацию к программному модулю «Очиститель», 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 «Очиститель»
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.

Очиститель – аппаратно-программное средство многоступенчатой очистки трафика от вредоносных составляющих и отправки пакетов очищенного трафика по назначению, осуществляющее непосредственную фильтрацию трафика.

Модуль Очиститель работает совместно с модулем Анализатор и, в зависимости от объема нагрузки на комплекс, могут быть поставлены в следующих вариантах:

- Совмещенный - Анализатор и Очиститель реализованы в рамках одного аппаратного модуля;
- Раздельный - Анализатор и Очиститель реализованы в рамках разных аппаратных модулей.

В случае необходимости очистки большего объема трафика, увеличение пропускной способности осуществляется за счет добавления модулей Очиститель.

3 Функциональные возможности

3.1 Функциональные возможности Модуля «Очиститель»

Модуль Очиститель взаимодействуют с Модулем Лидер и получает от него команды для обработки проходящего трафика

Модуль Очиститель имеет разные режимы работы:

- BGP-ответвление;
- L2-мост;
- ARP-спуфинг.

Модуль Очиститель может работать в режиме «сенсор», позволяющем выявлять аномалии, получая копию входящего и(или) исходящего трафика защищаемой сети.

Работа в режиме сенсора необходима в следующих случаях:

- в сети отсутствуют источники netflow, необходимые для работы модуля Анализатор. В качестве источника netflow выступает модуль Очиститель;
- необходимо проводить постоянный детализированный анализ трафика на уровне протоколов приложений для отдельных хостов или защищаемой сети в целом.

Работа модуля Очиститель в режиме сенсора позволяет:

1. подавать на модуль Анализатор информацию о трафике, поступающем на сенсор, по протоколу netflow;
2. выполнять статистический анализ подаваемого на сенсор HTTP-трафика с помощью методов HTTP-журнал и HTTP-анализ;
3. осуществлять анализ трафика почтовых серверов на предмет ошибок авторизации и большого числа получателей и формировать черный список хостов, выполняющих опасные действия или участвующих в массовых рассылках;
4. просматривать «сырой трафик», поступающий на сенсор, с учетом заданных критериев фильтрации, а также осуществлять выгрузку данного трафика в формате pcap.

При выборе и реализации варианта включения, обеспечивается возможность перенаправления трафика на очистку и возврат очищенного трафика обратно в сеть.

Взаимодействие с Модулем Очиститель осуществляется по протоколу SSH.

3.2 Функциональные возможности компонентов Модуля «Очиститель»

- компонент осуществляющий фильтрацию трафика и его очистку от вредоносной составляющей;
- компонент отслеживающий сетевые подключения к подсистемам Анализатор и Очиститель и уведомляющий о неразрешенных подключениях;
- компонент реализующий контроль целостности собственных компонентов.

3.3 Интерфейсы Модуля «Очиститель»

Очиститель имеет интерфейс взаимодействия с модулем Анализатор и высокоскоростные интерфейсы для очистки трафика.

3.4 Аппаратная реализация

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

3.5 Программная реализация

Модуль «Очиститель» устанавливается в среде функционирования операционной системы Debian 10.

4 Работа с Очистителем

Настройка и управление работы Модуля Очиститель производится из Модуля Анализатор, либо (если установлен) из Модуля Лидер.

Доступены следующие функциональные возможности:

- добавление Очистителя
- редактирование настроек
- проверка работоспособности
- удаление очистителя
- сбор DPI статистики
- управление функцией аппаратного байпаса
- использование групповой очистки
- балансировка нагрузки между модулями очистки в составе группы очистителей