ООО "Гарда Технологии"

Функциональная спецификация

ПК "Периметр"

Нижний Новгород, 2022

Оглавление

1 Введение

1.1 Аннотация

Данный документ представляет собой Функциональную спецификацию 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
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, который 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 Функциональные возможности

3.1 Функциональные возможности Модуля «Анализатор»

Модуль Анализатор взаимодействуют с модулем Лидер, с маршрутизирующим оборудованием сети и осуществляют отправку команд на модули Очиститель. Анализаторы могут работать в режиме горячего резерва (1+1).

- выполняет мониторинг трафика СПД и выявляет аномалии;
- осуществляет непрерывный анализ трафика контролируемой сети;
- при обнаружении атаки выдает команды маршрутизирующему оборудованию на первичную очистку и последующее перенаправление трафика на Очиститель
- в случае автономной реализации (без модуля Лидер):
  - обеспечивает веб-интерфейс
  - обеспечивает аутентификацию пользователей
  - обеспечивает ролевую модель и разграничение прав доступа
  - обеспечивает управление (администрирование) ПК
  - обеспечивает регистрация событий и сигнализацию
  - обеспечивает резервирование подсистем ПК

3.2 Функциональные возможности компонентов Модуля «Анализатор»

- контролируют работоспособность всех остальных модулей и перезапускает при необходимости.
- обеспечивают запись потока «сырых» netflow записей в Хранилище.
- обеспечивают возможность взаимодействия с другим программным комплексом «Периметр» в рамках передачи запросов на включение фильтрации. Позволяет остановить или запустить задание подавления, загрузить черный/белый список, изменить защищаемые префиксы на центральной системе.
- обеспечивают возможность логирования событий.
- обеспечивают проверку целостности программного обеспечения, обновлений базы решающих правил, параметров настройки и хранимых данных, позволяет обеспечить контроль целостности и/или выявление фактов нелегитимного внесения изменений.
- обеспечивают возможность отслеживания сетевых подключений и уведомления о неразрешенных подключениях.
- обеспечивают механизмы синхронизации. Находясь на резервной машине вытягивает данные с активной машины, копирует недостающие данные отчетов, также удаляет данные, которые уже отсутствуют на активной машине.
- обеспечивают взаимодействие с DNS серверами в рамках разрешения доменных имен.

- обеспечивают проверку доступности сервисов.

3.3 Интерфейсы Модуля «Анализатор»

Модуль Анализатор имеет 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.

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

Анализатор автоматически определяет интерфейсы контролируемой СПД. Для этого служат данные NetFlow-датаграмм и данные, полученные в результате периодического опроса маршрутизаторов по протоколу SNMP.

Определяются следующие данные:

- название маршрутизатора, которому принадлежит интерфейс;
- snmp-индекс интерфейса на маршрутизаторе;
- название интерфейса;
- описание интерфейса;
- скорость передачи данных через интерфейс;
- IP-адрес, настроенный на интерфейсе;
- ASN соседа - ASN автономной системы соседней сети, к которой подключен интерфейс;
- тип интерфейса - тип, который определенный в раках классификации интерфейсов;
- правило автоклассификации, в соответствии с которым был определён тип интерфейса;
- отчёт NetFlow - кнопка, при нажатии на которую, осуществляется переход на страницу детального отчёта по трафику через интерфейс из данных, полученных по протоколу NetFlow;
- отчёт SNMP - кнопка, при нажатии на которую, осуществляется переход на страницу детального отчёта по трафику через интерфейс из данных, полученных по протоколу SNMP;
- наименование модуля Анализатор, с которым взаимодействует маршрутизатор.

3.4 Дополнительные возможности

3.4.1 Сигнатуры зловредного трафика

Сигнатура - это набор специфических признаков, характеризующих трафик.

Детектирование аномального трафика по сигнатурам зловредного трафика основывается на возможности сопоставления трафика наблюдаемого объекта или отдельного хоста с трафиком, определяемым другим наблюдаемым объектом.

Этот принцип позволяет детектировать наличие или превышение порога для трафика, соответствующего одновременно наблюдаемому объекту (хосту наблюдаемого объекта) и дополнительному наблюдаемому объекту, задаваемому, как правило, критерием сопоставления «Ботсеть» и содержащим актуальные списки узлов ботсетей, распространителей вредоносного контента, сетевых сканеров, уязвимых серверов, а также иных узлов, использующихся в качестве источников DDoS атак.

3.5 Аппаратная реализация

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

3.6 Программная реализация

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

Модуль «Анализатор» может устанавливаться в виртуальной среде. Требования к ресурсам платформы виртуализации аналогичны аппаратным характеристикам. При установке Изделия на платформе виртуализации необходимо обеспечить наличие выделенных физических Ethernet-портов для приема трафика.

4 Работа с Анализатором

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

4.1 Управление ПК через WEB

Модуль «Анализатор» поддерживает работу комплекса через WEB. Позволяет идентифицировать и аутентифицировать пользователей, управлять их учетными записями, блокировать сеанса доступа к комплексу при неактивности пользователя, настраивать комплекс, собирать, записывать и хранить информацию о событиях безопасности, просматривать результаты событий безопасности и реагировать на них, проводить контроль и анализ сетевого трафика, обнаруживать идентифицировать и регистрировать инциденты в информационной системе, информировать о компьютерных инцидентах и проводить их анализ, записывать в журнал информацию о состоянии комплекса и событиях безопасности.

4.2 Управление ПК через JSON RPC API

Программный интерфейс удалённого администрирования (API) позволяет управлять работой и осуществлять настройку удалённо по протоколу JSON-RPC, работающему поверх HTTPS

4.3 Управление ПК через CLI

Интерфейс командной строки (command line interface, CLI) позволяет управлять работой и осуществлять настройку ПК удалённо по протоколу SSH в интерактивном режиме.