ООО "Гарда Технологии"

Функциональная спецификация

Модуль Лидер ПК "Периметр"

Нижний Новгород, 2022

Оглавление

1 Введение

1.1 Аннотация

Данный документ представляет собой Функциональную спецификацию 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
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 Функциональные возможности

2.1 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 «Лидер» является центром управления всего комплекса, предоставляющем интерфейс управления пользователя.

Модуль «Лидер» осуществляет сбор и агрегацию всей информации, предоставляемой анализаторами ПК «Периметр», а также предоставляет инструменты для настройки и управления подсистемами анализа и очистки.

2.2 Функциональные возможности

2.2.1 Функциональные возможности Модуля «Лидер»

- 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
- 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

2.2.2 Функциональные возможности компонентов Модуля

- synmond контролирует работоспособность всех остальных модулей и перезапускает при необходимости.
- synnetflowd обеспечивает запись потока «сырых» netflow записей в Хранилище.
- synsigd обеспечивает 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.
- synrlogd обеспечивает возможность логирования событий.
- ta-synverify обеспечивает проверку целостности программного обеспечения, обновлений базы решающих правил, параметров настройки и хранимых данных, позволяет обеспечить контроль целостности и/или выявление фактов нелегитимного внесения изменений.
- tc-synsecd обеспечивает возможность отслеживания сетевых подключений и уведомления о неразрешенных подключениях.
- syn1p1 обеспечивает механизмы синхронизации. Находясь на резервной машине вытягивает данные с активной машины, копирует недостающие данные отчетов, также удаляет данные, которые уже отсутствуют на активной машине.
- syndnsd обеспечивает взаимодействие с DNS серверами в рамках разрешения доменных имен.
- synhbd обеспечивает проверку доступности сервисов.
- www поддерживает работу комплекса через WEB, API и CLI. 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.

2.3 Интерфейсы Модуля «Лидер»

Модуль Лидер имеет 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.

2.4 Дополнительные возможности

2.4.1 Управление ПК через JSON RPC API

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

2.4.2 Выполнение команд через API

Управление ПК при помощи API можно реализовать посредством утилиты curl. Для этого:

- создается текстовый файл в формате txt, в который записывается команда или сценарий команд. Каждая отдельная команда сценария команд записывается с новой строки.
- текстовый файл передается ПК на исполнение при помощи служебной программы командной строки с URL.

2.5 Аппаратная реализация

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

2.6 Программная реализация

Все подсистемы ПК «Периметр» устанавливаются в среде функционирования операционной системы Debian 10. Также подсистему хранения данных допускается устанавливать в среде функционирования операционной системы Альт 8 СП.

ПК «Периметр» 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.

3 Работа с Лидером

3.1 Рабочее Место Пользователя Системы

Графический интерфейс Пользователя Системы выполнен в виде веб-приложения. Доступ к интерфейсу осуществляется с использованием веб-браузеров:

- Google Chrome версии 102.0.5005.115 и выше;
- Mozilla Firefox 101.0.1 и выше;
- Opera 75.0.3969.171 и выше.

Не поддерживается работа браузера Internet Explorer в режиме совместимости.

Операционная система, на которой запускается веб-браузер, может быть любой из поддерживаемых конкретной версией браузера.