ГАРДА
ТЕХНОЛОГИИ

ООО "Гарда Технологии"

Руководство администратора

Модуль Очиститель ПК "Периметр"

Нижний Новгород, 2022

Оглавление

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство администратора 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
БРП	База решающих правил
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 Установка модуля «Очиститель»

3.1 Развертывание комплекса

В рамках развертывания комплекса необходимо произвести приемку согласно комплектности поставки и проверку информации, записанной на оптический диск установочного комплекта.

Для функционирования ПК «Периметр» необходимо установить операционную систему Debian 10.0. Дистрибутив доступен на официальном сайте (https://cdimage.debian.org/cdimage/archive/10.7.0/amd64/iso-cd/). Поддерживаемая архитектура - amd64, поддерживаемая версия ядра системы - 4.19.0-6-amd64.

Действия по формированию функциональной среды требуют наличие прав суперпользователя.

После разметки дискового пространства и установки необходимых для функционирования используемой аппаратной платформы драйверов и утилит, выполняется установка модуля «Очиститель» с помощью менеджера пакетов:

```
apt-get install --assume-yes --allow-unauthenticated -o DPkg::Options::="--force-overwrite
↪" syntc-dpdk
```

После установки модуля «Очиститель» все его компоненты запускаются автоматически.

3.2 Первоначальная настройка модуля «Очиститель»

Для первоначальной настройки:

1. Определите номера интерфейсов Очистителя, которые будут использоваться в качестве входных и выходных при очистке трафика (входной и выходной интерфейсы должны располагаться на одной плате PCIE).
2. Выполните настройку интерфейсов на использование DPDK.
3. При необходимости выполните дополнительную настройку Очистителя согласно рекомендациям индивидуального технического решения по интеграции Комплекса .

3.3 Контроль старта модуля «Очиститель»

Контроль старта производится из Web-интерфейса модуля Анализатор либо модуля Лидер (если он установлен).

Для контроля старта необходимо:

- Перейти на экран «Администрирование / Подавление атак / Управление очистителями»;
- Убедиться, что все модули Очиститель запущены.

4 Настройка модуля «Очиститель»

Настройка производится из Web-интерфейса модуля Анализатор либо модуля Лидер (если он установлен).

Все очистители, включенные в состав комплекса, представлены на странице управления очистителями «Администрирование / Подавление атак / Управление очистителями». На данном экране присутствует фильтр для выбора очистителей по заданным критериям и список очистителей в виде таблицы со следующими полями:

- поле для выделения необходимого очистителя;
- Название – наименование модуля, дополнительно в поле отображается количество активных заданий очистки;
- Описание – дополнительная информация о модуле;
- IP-адрес – адрес управления модулем, так же если возможно определить доменное имя, оно будет отображено в этом поле;
- Конфигурация – информация о режиме работы очистителя и наборе маршрутизаторов, с которых на него перенаправляется трафик;
- Состояние – статус модуля:
  - «Не работал» – очиститель настроен в системе, но подключен не был;
  - «Неизвестно» – состояние очистителя неизвестно, наведя курсор мыши на пиктограмму можно уточнить причину, которая может быть одной из следующих:
    * анализатор, к которому подключен очиститель, не установлен;
    * анализатор, к которому подключен очиститель, отключен;
    * анализатор, к которому подключен очиститель, не в сети;
  - «Запущен» – очиститель настроен в системе и находится на связи с анализатором;
- Анализатор – название и состояние модуля Анализатор, который управляет Очистителем;
- Режим Bypass – управление функцией аппаратного байпаса:
  - Активный – сетевые адаптеры очистителя находятся в активном состоянии и пропускают трафик на очистку;
  - Холостой – сетевые адаптеры очистителя находятся в режиме bypass, трафик в очиститель не подается;
  - Не поддерживается – сетевые адаптеры очистителя не поддерживают функцию аппаратного bypass.

Ниже списка зарегистрированных Очистителей находятся кнопки управления:

- Добавить очиститель – переход в форму добавления связи с новым Очистителем;
- Удалить выбранные – удаление связи с выбранными в списке Очистителями;
- Сырой трафик – запуск технологического сбора «сырого трафика» на выбранных Очистителях для поиска и просмотра трафика, который проходит через Очистители, но не попадает в активные задания подавления.

4.1 Добавление очистителя

Добавление очистителя происходит в зависимости от режима его работы:

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

4.1.1 Схема подключения «BGP-ответвление»

Чтобы добавить очиститель, подключенный по схеме «BGP-ответвление» необходимо:

1. перейти на страницу управления очистителями «Администрирование / Подавление атак / Управление очистителями»;
2. нажать на кнопку «Добавить очиститель»;
3. на открывшейся странице добавления очистителя заполнить поля:
    - на вкладке «Описание»:
        - в поле «Название» указать название добавляемого очистителя;
        - при необходимости в поле «Описание» указать описание добавляемого очистителя;
        - в поле «IP-адрес интерфейса управления» и «порт» задать IP-адрес и порт управления добавляемым очистителем;
        - выбрать Анализатор, к которому будет привязан очиститель;
        - установить параметр «Разрешить установку соединения с очистителем» для включения соединения анализатора и очистителя;
        - при необходимости установить параметр «Вести мониторинг сетевых подключений», для включения контроля за сетевыми подключениями;
        - при необходимости установить параметр «Загружать SSL сертификаты», для включения загрузки SSL/TLS ключей, используемых при перехвате шифрованного трафика в очистителе;
        - при необходимости установить параметр «Останавливать задания очистки при разрыве соединения с очистителем » для остановки заданий, связанных с очистителем, в случае его недоступности;
    - на вкладке «Схема включения» в одноименном поле выбрать вариант «BGP-ответвление»;
    - на вкладке «Интерфейсы»:
        - В поле «IP-адрес входного интерфейса» указать IPv4 и/или IPv6 адрес входящего интерфейса очистителя, на который будет перенаправляться трафик на очистку;
        - В поле «IP-адрес выходного интерфейса» указать IPv4 и/или IPv6 адрес исходящего интерфейса очистителя, с которого очищенный трафик будет отправляться в сеть;

  - В поле «IP-адрес next-hop» указать IPv4 и/или IPv6 адрес следующей точки маршрута, на которую будет перенаправляться очищенный трафик;
  - При необходимости в поле «MAC-адрес IP next-hop» указать аппаратные адреса следующих точек маршрута по IPv4 и IPv6 протоколам. В данном случае разрешение данных адресов происходить не будет;

  Примечание: в случае использования протокола IPv4 или IPv6 все поля адресов, относящихся к данному протоколу, должны быть заполнены. Не допускается заполнение не всех полей, например, заполнение входящего адреса по протоколу IPv4, а исходящего адреса по протоколу IPv6.

- на вкладке «BGP»:
  - нажать на кнопку «Выбрать»;
  - в открывшемся списке указать маршрутизаторы, на которые необходимо отправлять BGP-анонсы по перенаправление трафика на добавляемый очиститель;
  - указать режим перенаправления трафика:
    * BGP offramp – стандартный анонс BGP;
    * Flowspec Route Target – анонс BGP flow specification с указанием действия redirect;
- на вкладке «Глобальный фильтр» находятся элементы настройки данного фильтра, но данные элементы управления доступны только при редактировании параметров очистителя и при его добавлении не используются;
- на вкладке «Sensor»:
  - при необходимости в разделе «Netflow v9» задать адрес и порт назначения передачи сформированных очистителем, на основании прошедшего через него трафика, данных Netflow. Дополнительным параметром является задание частоты сэмплирования. Для задания автоматического определения частоты сэмплирования - установить его значение равное 0;
  - при необходимости включения функции сбора DPI данных (по протоколам DNS, VoIP, POP3, SMTP, IMAP4) - задать адрес и порт получателя данных. В качестве получателя должен выступать либо анализатор, который в дальнейшем будет применять полученные данные в работе, либо внешняя система сбора и анализа DPI данных;
- на вкладке «DPI Flow» ввести параметры получателей информации о трафике, руководствуясь пунктом «Сбор DPI статистики» настоящего руководства;
- на вкладке «GRE»:
  - при необходимости передачи очищенного трафика в GRE-туннель - установить параметр «Инкапсуляция GRE» в разделе IPv4 и/или IPv6 графе;
  - указать значение параметра «Внутренний IP-адрес GRE туннеля (со стороны очистителя)»;
  - указать значение параметра «IP-адрес конечной точки GRE туннеля» (с которым будет устанавливаться туннелирование);

  Примечание: в качестве внешнего адреса туннеля со стороны очистителя будет выступать адрес исходящего интерфейса;

- на вкладке «Параметры оборудования» ввести параметры модуля Очиститель, которые будут использоваться при динамическом управлении параметрами очистки в зависимости от мощности атаки, руководствуясь пунктом «Параметры групповой очистки» настоящего руководства;
- на вкладке «Журнал динамического черного списка» включить флаг, если необходимо сохранять информацию о работе метод «Динамический черный список» на очистителе;

4. нажать кнопку «Сохранить».

4.1.2 Схема подключения «L2-мост»

Чтобы добавить очиститель, подключенный по схеме «L2-мост» необходимо:

1. перейти на страницу управления очистителями «Администрирование / Подавление атак / Управление очистителями»;
2. нажать на кнопку «Добавить очиститель»;
3. на открывшейся странице добавления очистителя заполнить поля:
   - на вкладке «Описание»:
     – в поле «Название» указать название добавляемого очистителя;
     – при необходимости в поле «Описание» указать описание добавляемого очистителя;
     – в поле «IP-адрес интерфейса управления» и «порт» задать IP-адрес и порт управления добавляемым очистителем;
     – выбрать Анализатор, к которому будет привязан очиститель;
     – установить параметр «Разрешить установку соединения с очистителем» для включения соединения анализатора и очистителя;
     – при необходимости установить параметр «Вести мониторинг сетевых подключений», для включения контроля за сетевыми подключениями;
     – при необходимости установить параметр «Загружать SSL сертификаты», для включения загрузки SSL/TLS ключей, используемых при перехвате шифрованного трафика в очистителе;
     – при необходимости установить параметр «Останавливать задания очистки при разрыве соединения с очистителем » для остановки заданий, связанных с очистителем, в случае его недоступности;
   - на вкладке «Схема включения» в одноименном поле выбрать вариант «L2-мост»;
   - на вкладке «Интерфейсы»:
     – в поле «IP-адрес next-hop» указать IPv4 и/или IPv6 адрес следующей точки маршрута, на которую будет перенаправляться очищенный трафик;

   Примечание: адрес next-hop задается в случае, когда очиститель не стоит в разрыве основного канала и требуется BGP-перенаправление трафика на очиститель. Если BGP-перенаправление не требуется, то адрес можно указать любой.

- при использовании перенаправления трафика на очистку, на вкладке «BGP»:
  - нажать на кнопку «Выбрать маршрутизаторы с поддержкой BGP»;
  - в открывшемся списке выбрать маршрутизаторы, на которые необходимо отправлять BGP-анонсы по перенаправление трафика на добавляемый очиститель;
  - указать режим перенаправления трафика:
    * BGP offramp – стандартный анонс BGP;
    * Flowspec Route Target – анонс BGP flow specification с указанием действия redirect;
- на вкладке «Глобальный фильтр» находятся элементы настройки данного фильтра, но данные элементы управления доступны только при редактировании параметров очистителя и при его добавлении не используются;
- на вкладке «Sensor»:
  - при необходимости в разделе «Netflow v9» задать адрес и порт назначения передачи сформированных очистителем, на основании прошедшего через него трафика, данных Netflow. Дополнительным параметром является задание частоты сэмплирования. Для задания автоматического определения частоты сэмплирования - установить его значение равное 0;
  - при необходимости включения функции сбора DPI данных (по протоколам DNS, VoIP, POP3, SMTP, IMAP4) - задать адрес и порт получателя данных. В качестве получателя должен выступать либо анализатор, который в дальнейшем будет применять полученные данные в работе, либо внешняя система сбора и анализа DPI данных;
- на вкладке «DPI Flow» ввести параметры получателей информации о трафике, руководствуясь пунктом «Сбор DPI статистики» настоящего руководства;
- на вкладке «Параметры оборудования» ввести параметры модуля Очиститель, которые будут использоваться при динамическом управлении параметрами очистки в зависимости от мощности атаки, руководствуясь пунктом «Параметры групповой очистки» настоящего руководства;
- на вкладке «Журнал динамического черного списка» включить флаг, если необходимо сохранять информацию о работе метод «Динамический черный список» на очистителе;

4. нажать кнопку «Сохранить».

4.1.3 Схема подключения с использованием технологии «ARP-спуфинг»

Чтобы добавить очиститель, с использованием технологии «ARP-спуфинг» необходимо:

1. перейти на страницу управления очистителями «Администрирование / Подавление атак / Управление очистителями»;
2. нажать на кнопку «Добавить очиститель»;
3. на открывшейся странице добавления очистителя заполнить поля:
   - на вкладке «Описание»:

- в поле «Название» указать название добавляемого очистителя;
- при необходимости в поле «Описание» указать описание добавляемого очистителя;
- в поле «IP-адрес интерфейса управления» и «порт» задать IP-адрес и порт управления добавляемым очистителем;
- выбрать Анализатор, к которому будет привязан очиститель;
- установить параметр «Разрешить установку соединения с очистителем» для включения соединения анализатора и очистителя;
- при необходимости установить параметр «Вести мониторинг сетевых подключений», для включения контроля за сетевыми подключениями;
- при необходимости установить параметр «Загружать SSL сертификаты», для включения загрузки SSL/TLS ключей, используемых при перехвате шифрованного трафика в очистителе;
- при необходимости установить параметр «Останавливать задания очистки при разрыве соединения с очистителем » для остановки заданий, связанных с очистителем, в случае его недоступности;

- на вкладке «Схема включения» в одноименном поле выбрать вариант «ARP-спуфинг»;
- на вкладке «Глобальный фильтр» находятся элементы настройки данного фильтра, но данные элементы управления доступны только при редактировании параметров очистителя и при его добавлении не используются;
- на вкладке «Sensor»:
  - при необходимости в разделе «Netflow v9» задать адрес и порт назначения передачи сформированных очистителем, на основании прошедшего через него трафика, данных Netflow. Дополнительным параметром является задание частоты сэмплирования. Для задания автоматического определения частоты сэмплирования - установить его значение равное 0;
  - при необходимости включения функции сбора DPI данных (по протоколам DNS, VoIP, POP3, SMTP, IMAP4) - задать адрес и порт получателя данных. В качестве получателя должен выступать либо анализатор, который в дальнейшем будет применять полученные данные в работе, либо внешняя система сбора и анализа DPI данных;
- на вкладке «DPI Flow» ввести параметры получателей информации о трафике, руководствуясь пунктом «Сбор DPI статистики» настоящего руководства;
- на вкладке «Параметры оборудования» ввести параметры модуля Очиститель, которые будут использоваться при динамическом управлении параметрами очистки в зависимости от мощности атаки, руководствуясь пунктом «Параметры групповой очистки» настоящего руководства;
- на вкладке «Журнал динамического черного списка» включить флаг, если необходимо сохранять информацию о работе метод «Динамический черный список» на очистителе;

4. нажать кнопку «Сохранить».

4.2 Редактирование настроек очистителя

Чтобы отредактировать настройки очистителя необходимо:

1. перейти на страницу управления очистителями «Администрирование / Подавление атак / Управление очистителями»;
2. щёлкните левой клавишей мыши по названию очистителя, в редактировании которого есть необходимость;
3. внести необходимые изменения, по аналогии с процедурой добавления;
4. нажать кнопку «Сохранить».

4.2.1 Настройка на вкладке «Глобальный фильтр»

Для каждого очистителя существует один глобальный фильтр, общий для всех заданий очистки на очистителе. Метод используется для формирования общих правил фильтрации, блокирования заведомо недопустимых префиксов сетей, неверных комбинаций флагов и других специфических параметров контролируемой сети.

Чтобы настроить метод «Глобальный фильтр» необходимо:

1. перейти на страницу управления очистителями «Администрирование / Подавление атак / Управление очистителями»;
2. щёлкнуть левой кнопкой мыши по названию очистителя;
3. перейти на закладку «Глобальный фильтр»;
4. нажать кнопку «Редактировать», после чего откроется диалоговое окно глобальные правила;
5. задать действия и сигнатуры трафика для всех заданий подавления на очистителе. Сделать это можно:
6. вручную, введя текст сигнатуры в поле;
7. воспользовавшись мастером правил, который вызывается нажатием кнопки «Добавить с помощью мастера»;
8. загрузив в поле редактирования список, определенный в меню Администрирование / Подавление атак / Глобальные настройки, нажав на кнопку «Загрузить стандартный список»;
9. вернуть сигнатуру, используемую на очистителе в данный момент, если необходимо откатить только что сделанные изменения, нажав на кнопки «Загрузить текущий список»;
10. нажать кнопку «Применить глобальный фильтр» для активации новых правил Очистителе.

Примечание: к настройке глобального фильтра необходимо относиться с осторожностью, так как все правила, заданные в нем, будут применены ко всем заданиям очистителя и могут повлиять на доступность защищаемых сервисов.

Вручную, либо с помощью «Мастера фильтров» можно сформировать параметры фильтрации:

- флаг NOT меняет условие на противоположное;
- адреса источников/получателей;
- порты источников/получателей;
- протоколы;
- тип сервиса (TOS);
- длина пакета;
- время жизни пакета (TTL);
- TCP-флаги;
- тип и код протокола ICMP/ICMPv6;
- страны/континенты;
- ethernet фильтр - выражается шестнадцатеричным значением и его смещением в сетевом пакете;
- IP фрагментация - пакет является IP фрагментом.

Допускается создание трех категорий правил:

- drop - правило – правило, при котором пакеты с заданными параметрами отбрасываются;
- pass - правило – правило, при котором пакеты с заданными параметрами пропускаются без анализа другими методами очистки;
- continue - правило – правило, при котором пакеты с заданными параметрами пропускаются через фильтр задания очистки и отправляются на анализ другими методами.

4.2.2 Настройка на вкладке «Sensor»

Sensor на очистителе выполняет функции:

- генерации потока Netflow данных на основании трафика, проходящего через интерфейсы очистителя (данная функция может быть полезна при отсутствии возможности получения Netflow данных с пограничных маршрутизирующих устройств, при условии, что трафик в защищаемую сеть проходит через интерфейсы очистителя в полном объеме);
- DPI-анализ на очистителе.

Для настройки генерации Netflow необходимо:

1. перейти на страницу управления очистителями «Администрирование / Подавление атак / Управление Очистителями»;
2. щёлкнуть левой кнопкой мыши по названию очистителя;
3. перейти на вкладку Sensor;
4. установить флажок «Включить» в разделе «Netflow v9»;
5. указать IP-адрес и порт назначения для передачи сгенерированного Netflow;
6. задать частоту сэмплирования. Если частота установлена в 0, то сэмплирование будет подбираться автоматически;

7. нажать на кнопку «Сохранить».

Для настройки DPI-анализа необходимо:

1. перейти на страницу управления очистителями «Администрирование / Подавление атак / Управление Очистителями»;
2. щёлкнуть левой кнопкой мыши по названию очистителя;
3. перейти на вкладку Sensor;
4. установить флажок «Включить» в разделе «Sensor»;
5. указать IP-адрес и порт назначения для передачи сгенерированных данных DPI;
6. нажать на кнопку «Сохранить».

4.3 Удаление очистителя

Чтобы удалить очиститель необходимо:

1. перейти на страницу управления очистителями «Администрирование / Подавление атак / Управление очистителями»;
2. установить флажки у очистителей, подлежащих удалению;
3. нажать кнопку «Удалить выбранные»;
4. подтвердить удаление, нажав кнопку «Да».

5 Обновление модуля «Очиститель»

Предприятие-разработчик на этапе сопровождения может осуществлять периодический выпуск обновлений.

Определены три типа обновлений Изделия:

- 1 тип – обновление баз данных, необходимые для поддержания актуальности БРП;
- 2 тип – обновление, направленное на устранение выявленных уязвимостей (критическое обновление) ПК;
- 3 тип – обновление, направленное на добавление и/или совершенствование реализации функций безопасности, на расширение числа поддерживаемых программных и аппаратных платформ (обновление версии ПК).

Информирование потребителей о выпуске обновлений Изделия 2 и 3 типа осуществляется путем рассылки информационных уведомлений потребителям Изделия.

Обновление модуля «Анализатор» осуществляется с помощью менеджера пакетов.