Техническая документация

Содержание

1. Назначение ПК "Гарда DPI"*

***Под ПК "Гарда DPI" понимается программное обеспечение «Система анализа трафика ADM S1».**

Программный комплекс "Гарда DPI" предназначен для глубокой инспекции и модификации трафика, на основании пользовательских политик:

1. Фильтрация интернет-ресурсов по ip-адресам, подсетям, hostname и URL.
    1. фильтрация по черным спискам - запрещено указанное
    2. фильтрация по белым спискам - запрещено не указанное
    3. исключение записей из фильтрации посредством списков исключений либо посредством указания статуса ресурса оператором
    4. фильтрация высокоприоритетных ресурсов - указание ресурсов, фильтрация которых берется под особый контроль
    5. загрузка списков ресурсов из внешних источников - sftp, api, госреестров (в том числе посредством дельт). Выгрузка списков фильтрации в файл.
    6. верификация загружаемых ресурсов на предмет корректности записей. Их автоматическое исправление, либо ожидание исправления и подтверждения оператором. Нормализация записей.
    7. функционал обогащения http-заголовков (в том числе, поддержка хеширования) запросов пользователя, с указанием MSISDN, для анализа принимающей стороной
    8. блокировка ресурсов посредством возврата html-страницы (код 200, 451), редиректа на указанный ресурс (код 302), тихой блокировки (rst), явное подтверждения перехода на ресурс пользователем
    9. визуальная статистика запросов пользователей, в том числе, заблокированных, с указанием причин блокировки
2. Фильтрация категорий интернет-ресурсов
    1. фильтрация по черным спискам - запрещено указанное

    2. фильтрация по белым спискам - запрещено не указанное
    3. исключение записей из фильтрации посредством списков исключений
    4. визуальная статистика запросов пользователей, в том числе, заблокированных, с указанием причин блокировки
3. Критерии матчинга трафика пользователя или группы пользователей по условиям: ip, приложение, порт, ресурс, URL, протокол присутствует в стеке запроса, user agent и т.д., с последующим применением политики к данному трафику:
    1. блокировка с разрывом соединения (rst)
    2. тихая блокировка (соединение блочится без посылки уведомлений)
    3. ухудшение трафика (имитация плохого соединения)
    4. обогащение ip уровня метками TC\DSCP
    5. обогащение tcp уровня флагом reserved bits или добавление tcp-опции фиксированного или динамического (user id, imsi, msisdn) значения с хешированием или без. Обогащение может применятся к пакетам с выбранными tcp флагами
4. Статическое (ip-адрес, vlan-тег) и динамическое (radius) определение пользователей в трафике
5. Защита абонентов от простых DOS\DDOS-атак
6. Анализ дропов и задержек пакетов абонента
7. Шейпинг трафика с указанием гарантированной и пиковой скоростей абонентов
8. Предоставление оператору веб-интерфейса для управления работой ПК

2. Программные и аппаратные требования к системе

- Система устанавливается на x86/amd64 сервер под управлением последних версий ПО Ubuntu lts.
- В сервере предусмотрено необходимое количество dpdk-совместимых сетевых интерфейсов согласно количеству обрабатываемых каналов трафика оператора.
- Два порта для менеджмента и ssh доступа
- В случае необходимости загрузки списков рос. реестров - серверу предоставлен доступ в интернет.

Референсная конфигурация

- 1 x Платформа 1U NCA-5520A LANNER
- 8 x Модуль памяти 32GB PC23400 ECC REG CT32G4RFD4293 CRUCIAL
- 1 x Процессор Intel Xeon 2100/35.75M S3647 OEM GOLD 6252 CD8069504194401 IN
- 2 x SSD жесткий диск SATA2.5" 240GB TLC D3-S4610 SSDSC2KG240G801 INTEL
- 4 x Модуль 10GBE SFP+ 4P PSE2110-10 NCS2-IXM407A LANNER
- 16 x TRANSCEIVER SFP+ E10GSFPSR 903239 INTEL

Лимиты обработки трафика для референсной конфигурации

- Пиковая нагрузка с минимальным функционалом:
    - packet size 128 bytes, 28 Mpps max

    - (500K IPv6 + 1M IPv4) fps
    - 110M Active flows
    - Latency ~ 130мкс
    - 20Gbps UL + 70Gbps DL
- Типовая нагрузка со стандартным функционалом, указанная на одно ядро. Нагрузка масштабируется по количеству ядер:
    - 6K fps / 1 Gbps
    - 724K sessions / 1 Gbps

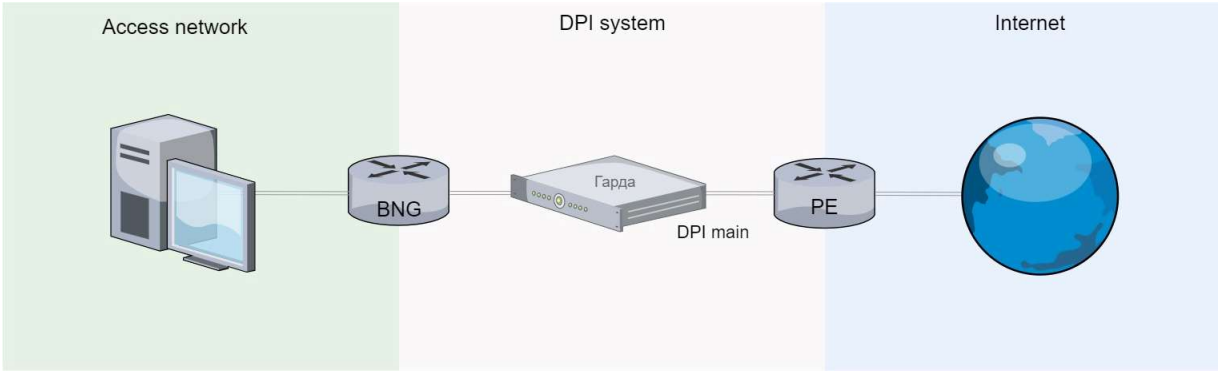
Виртуализация

В качестве системы виртуализации может использоваться любая, поддерживающая очереди на виртуализированных интерфейсах. Таковой является любая современная система виртуализации.

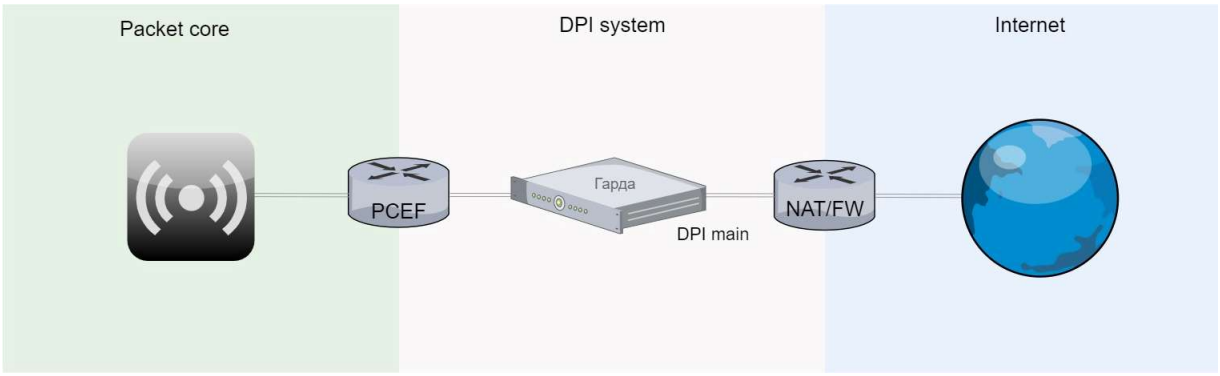
3. Схемы включения

Типовое размещение DPI в сети оператора - непосредственно перед шлюзом доступа в сеть Интернет. При таком включении требуется два порта на канал трафика. Количество каналов ограничено количеством сетевых карт в сервере:

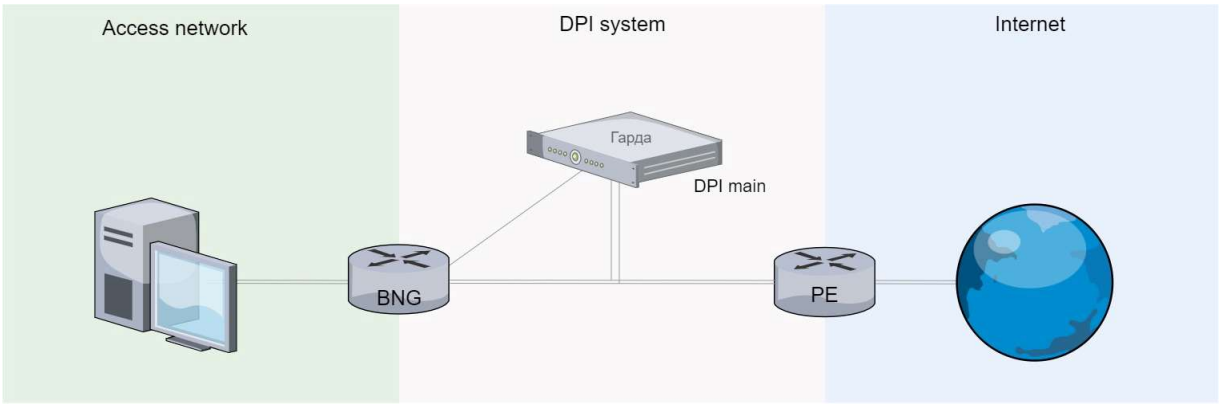
Сеть оператора ШПД:



Сеть мобильного оператора связи:

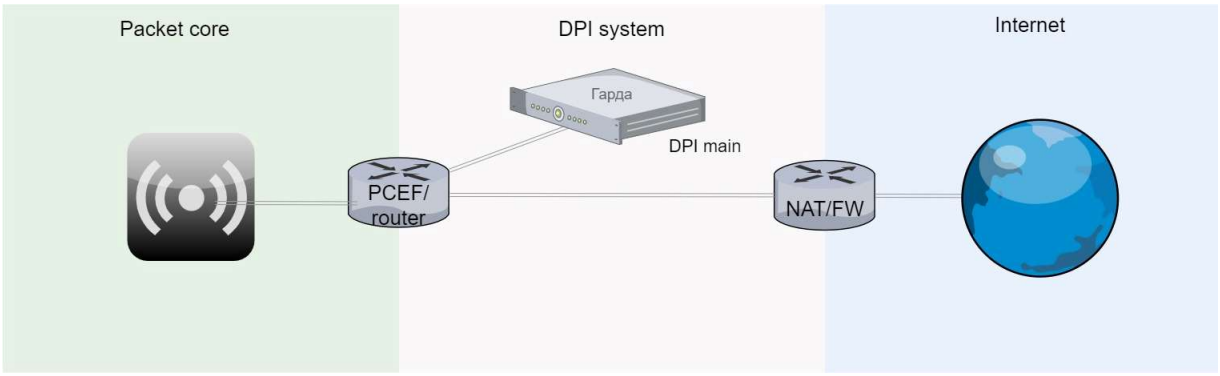


Так же возможно включение на копии трафика. DPI формирует ответы на копии клиентских запросов, которые возвращаются к клиенту:



Для функционала фильтрации трафика по спискам ресурсов, DPI достаточно UPLINK канала трафика.

Дополнительно DPI может быть интегрирована в сеть как VAS-платформа. При таком включении требуется один порт на канал трафика:



Помимо портов включения в сеть оператора, для работы DPI требуется минимум два медных порта – интерфейс IPMI для дистанционного управления сервером, а также

интерфейс SSH для удаленного доступа, скачивания списков госреестра, передачи статистики.

4. Механизмы резервирования

Сервера DPI резервируются по схеме Active-Active, Active-Standby, либо посредством балансировки трафика между нодами DPI. В случае резервирования Active-Standby на standby-серверах устанавливается сетевая карта с Bypass для обработки трафика в случае отказа основного и резервного маршрута одновременно. В случае отсутствия резервирования маршрутов (два независимых маршрута) сетевая карта с функцией резервирования (bypass) устанавливается в каждый сервер. Резервирование канала без перехода на резервный канал выполняется замыканием модуля bypass, встроенного в сетевую карту сервера.

5. Мониторинг

В случае аварии какой-либо из подсистем Гарда DPI, ПК информирует операторов о наличии проблемы и степени ее критичности.

<u>В задачи мониторинга входит оповещение в следующих случаях:</u>

- Отключение сервера
- Падение ПО подсистемы обработки, подсистемы управления или базы данных конфигурации и статистики
- Нехватка производительности подсистемы обработки трафика
- Превышение допустимого количества потерь на интерфейсах подсистемы обработки трафика
- Снижение объема трафика на интерфейсах подсистемы обработки ниже допустимого предела
- Пропадание связи подсистемы обработки трафика с базой данных конфигурации и статистики
- Пропадание связи подсистемы управления с подсистемой обработки трафика и с базой данных конфигурации и статистики
- Переход трафика на обходной путь \ bypass
- Переполнение разделов жестких дисков
- Превышение допустимого порога использования оперативной памяти
- Нехватка ресурсов центрального процессора
- Превышение допустимой температуры центрального процессора
- Отказ кулера
- Отказ жесткого диска

Оповещения об авариях доставляются путем передачи SMS на SMS-шлюз оператора или на электронную почту с помощью почтового сервера оператора. Оповещение о критических авариях осуществляются с помощью SNMP мониторинга, путем доставки

оператору SNMP трапов. Помимо этого, состояние системы можно анализировать в окне внешней системы мониторинга Zabbix.

6. Техподдержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании "Гарда Технологии": dpi.support@gardatech.ru