ООО «НТЦ ПРОТЕЙ»

СИСТЕМА ГЛУБОКОГО АНАЛИЗА И ПРИМЕНЕНИЯ ПОЛИТИК ДЛЯ УПРАВЛЕНИЯ ПАКЕТНЫМ ТРАФИКОМ PROTEI_DPI

Описание функциональных характеристик программного обеспечения и информация для установки и эксплуатации

Санкт-Петербург
2017

ОГЛАВЛЕНИЕ

ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Основные понятия и определения приведены в таблице 1.

Таблица 1. Термины и сокращения

Термин	Описание
АФ	Аппаратный Фильтр - компонент DPI, выполняющий низкоуровневую работу с пакетами и подсчет статистики
УС	Управляющий Сервер - программный компонент DPI, управляющий работой АФ
СОРМ	Система Оперативно-Розыскных Мероприятий
CDR	Charging Data Record -тарификационная запись данных
DDoS	Distributed Denial of Service - распределенная атака типа «отказ в обслуживании»
Diameter	Сеансовый протокол, обеспечивает взаимодействие между клиентами в целях аутентификации, авторизации и учёта различных сервисов (AAA, англ. authentication, authorization, accounting)
DPI	Deep Packet Inspection - глубокий анализ трафика
Gx	Интерфейс между элементами биллинг систем для контроля потребления трафика по протоколу Diameter (интерфейс описан в стандарте 3GPP)
Gy	Интерфейс для тарификация в реальном времени по протоколу Diameter (интерфейс описан в стандарте 3GPP)
OSI	Open System Interconnection - взаимодействие открытых систем
Radius	Remote Authentication in Dial-In User Service - протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между центральной платформой и оборудованием
PCRF	Policy and Charging Rules Function - функция политик и правил тарификации

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Обозначение и наименование программного обеспечения

Полное наименование: **Система глубокого анализа и применения политик для управления пакетным трафиком PROTEI_DPI**.

Условное обозначение PROTEI_DPI.

1.2 Техническая поддержка

Техническая поддержка, а также дополнительное консультирование по вопросам, возникающим в процессе установки и эксплуатации программного обеспечения, осуществляются производителем и службой технической поддержки.

1.2.1 Производитель

ООО «НТЦ ПРОТЕЙ»

194044, Санкт-Петербург

Большой Сампсониевский пр., д. 60, лит. А

Бизнес-центр «Телеком СПб»

Тел.: (812) 449-47-27

Факс: (812) 449-47-29

WEB: http://www.protei.ru

E-mail: info@protei.ru

1.2.2 Служба технической поддержки

ООО «НТЦ ПРОТЕЙ»

194044, Санкт-Петербург

Большой Сампсониевский пр., д. 60, лит. А

Бизнес-центр «Телеком СПб»

Тел.: (812) 449-47-27 доп. 5777 (круглосуточно)

Факс: (812) 449-47-29

WEB: http://www.protei.ru

E-mail: support.callcenter@protei.ru

1.3 Назначение и область применения

Система глубокого анализа трафика PROTEI_DPI - это современная система интеллектуального управления трафиком, предоставляющая возможность анализировать расход потоков данных и на основании собранной информации и требуемой политики предоставления сервиса распределять и оптимизировать трафик.

Система предназначена для использования на сетях провайдеров услуг мобильного или фиксированного широкополосного доступа (ШПД).

2 ОПИСАНИЕ ФУНКЦИОНАЛЬНОСТИ

2.1 Функциональные характеристики PROTEI_DPI

Программное обеспечение PROTEI_DPI представляет собой программный комплекс глубокого анализа трафика. С точки зрения архитектуры сети передачи данных, PROTEI_DPI является вынесенной системой глубокого анализа трафика (standalone DPI)

PROTEI_DPI обладает следующими функциональными характеристиками:

1. Глубокий анализ трафика в сети оператора на принадлежность к определённому сервису.

Система PROTEI_DPI устанавливается в сеть оператора-провайдера услуг как L2 устройство (на 2м уровне) и работает с трафиком на всех уровнях модели OSI, включая прикладной. Это позволяет анализировать абонентский трафик всех проходящих пакетов через сеть провайдера по следующим критериям:

- анализ трафика на принадлежность пакета определённому приложению по шаблонам, заголовкам, структурам данных, номерам портов;
- анализ последовательности пакетов, обладающих одинаковыми признаками, такими как IP адрес и порт источника, IP адрес и порт получателя, размер пакета, частота открытия новых сессий в единицу времени и т.д.;
- анализ трафика за счёт сбора статистики с разбивкой по приложениям, по тарифным планам, по регионам, по типам абонентских устройств;
- детектирование протоколов уровня приложений для широкого спектра сервисов: в том числе игровых протоколов, протоколов файлового обмена, протоколов почтового обмена, мгновенных сообщений, голосовых и видео вызовов и других.

2. Управление трафиком.

Система PROTEI_DPI позволяет управлять трафиком в сети провайдера с целью оптимального использования сетевых ресурсов:

- распределять полосу пропускания канала передачи данных. ограничение или перераспределение полосы пропускания может выполняться в соответствии с политикой, применяемой к определенным приложениям (протоколам) или в соответствии с

политикой обслуживания абонента (группы абонентов);

- применять политики обслуживания и правила тарификации в зависимости от даты и времени суток;
- фильтровать ресурсы на основе подгружаемого списка запрещенных ресурсов, а также по запросу внешнего хранилища;
- выполнять тарификацию потоков данных в реальном времени;
- блокировать вредоносный трафик;
- выполнять учет трафика с привязкой к протоколам и услугам;
- выполнять генерацию cdr и статических отчетов;
- выполнять применение политик обслуживания и правил тарификации, полученных из сервера политик (PCRF);
- перенаправлять трафик группы абонентов, подписанных на ту или иную дополнительную услугу, на внешние сервера;
- выполнять обнаружение и противодействие атакам DDoS двух типов:
  - syn-flood атака;
  - flood-атака.

3. Гибкая настройка трафика и политики предоставления сервиса.

В целях управления трафиком и настройки политики сервиса предоставляется графический интерфейс, позволяющий Провайдеру конфигурировать и анализировать трафик:

- создавать сигнатуры трафика, произвольные классификаторы протоколов и приложений;
- устанавливать приоритеты на скорость передачи трафика и ограничение полосы пропускания трафика на основе информации о протоколе уровня приложений;
- блокировать или разрешать необходимые сервисы, путем ведения черных и белых списков URL;
- ограничивать доступ к необходимым ресурсам путем блокировки сайтов по доменным номерам. Предоставляется возможность настраивать белые списки IP-адресов DNS-серверов, если адрес DNS не входит в белый список, поток данных от него блокируется;
- устанавливать расписания действия черных и белых списков;
- выполнять управление потоками данных в соответствии с

параметрами абонентского профиля на основе информации об абоненте, путем связывания потоков данных и идентификаторов абонентов с использованием протоколов RADIUS и Diameter;

- настраивать уведомления и условия отправки сообщений абонентам;
- формировать и просматривать статистические отчеты.

4. Поддержка интерфейсов взаимодействия с внешними системами.

Система PROTEI_DPI оснащена следующими внешними интерфейсами:

- RADIUS и Diameter для связывания IP-адреса и идентификатора абонента;
- 3GPP Gx к серверу политик и правил тарификации (PCRF);
- 3GPP Gy к системе тарификации в режиме реального времени;
- SNMP с поддержкой методов Get и Trap к системе мониторинга;
- CDR в формате CSV с возможностью выгрузки по FTP, sFTP, SCP, в базу данных;
- HTTP / XML к системе online-статистики.

5. Резервирование программных компонент.

В системе предусмотрено резервирование программных компонент. В системе организовано 2 типа резервирования:

- режим распределения нагрузки. в данном режиме все программные компоненты обрабатывают трафик. При выходе из строя одного из компоненты его трафик переводится на другие оставшиеся в работе;
- режим работы по схеме master-slave (active-standby). при выходе из строя одного из активных компонент его трафик начинают обрабатывать другие оставшиеся в работе компоненты.

2.2 Структура ПО PROTEI_DPI с описанием функциональности каждого компонента

Программное обеспечение PROTEI_DPI имеет модульную структуру (см. Рисунок 1).

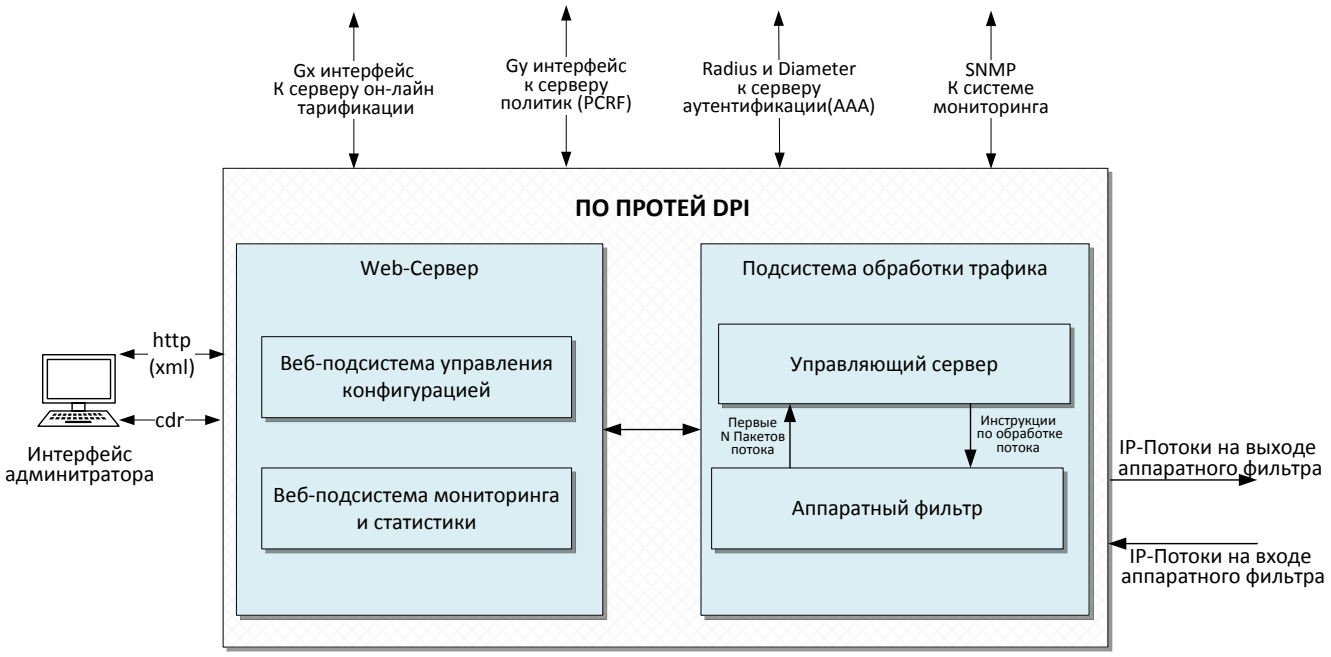

Рисунок 1. Структура программного обеспечения PROTEI_DPI

Система включает в себя следующие программные компоненты:

1. Веб-подсистема управления конфигурацией.

Предназначена для конфигурации протоколов, сервисов, тарифных планов и политик предоставления сервиса.

2. Веб-подсистема мониторинга и статистики.

Предназначена для контроля загрузки каналов передачи данных с разделением информации по протоколам и услугам, а также для генерации статистических отчетов за произвольный промежуток времени по произвольной выборке данных.

3. Подсистема обработки трафика.

Выполняет обработку потоков данных, а также обеспечивает взаимодействие с внешними платформами операторской сети, в том числе системой тарификации в режиме реального времени OCS, а также с сервером управления политикой и тарификацией PCRF.

Подсистема обработки трафика состоит из двух программных модулей — аппаратного фильтра и управляющего сервера.

Аппаратный фильтр (далее по тексту АФ) обрабатывает потоки данных на уровне пакетов. Анализируя такие параметры пакета, как IP-адрес источника, IP-адрес получателя, порт источника, порт получателя и протокол транспортного уровня, аппаратный фильтр объединяет передаваемые пакеты в логические единицы — потоки. По команде управляющего сервера, аппаратный фильтр управляет битрейтом потока, маркирует пакеты, а также ведет подсчет переданных в рамках потока байт.

Управляющий сервер (далее по тексту УС) путем разбора полученных от аппаратного фильтра n-первых пакетов потока до прикладного уровня модели OSI, определяет протокол и услугу, к которой относится поток, а также инициировавшего поток абонента. Обращаясь к серверу политик, правилам тарификации и в соответствии с локальной конфигурацией, УС определяет правила обслуживания потока и передает их на АФ. УС периодически считывает статистические счетчики по открытым потокам и передает информацию о потреблении трафика и о правилах тарификации на сервер политик через интерфейс Gx. Для выполнения кредитного контроля в режиме реального времени управляющий сервер оснащен интерфейсом Gy.

3 ТРЕБОВАНИЯ К ТЕХНИЧЕСКИМ СРЕДСТВАМ ДЛЯ УСТАНОВКИ И ЭКСПЛУАТАЦИИ ПО

Технические средства предоставляет Заказчик ПО.

Для эксплуатации системы необходимы промышленные сервера, на которые инсталлируются компоненты системы и автоматизированное рабочее место для администрирования.

Сервера и терминал пользователя должны быть соединены по сети.

Количество серверов, на которых располагается система, зависит от необходимой ёмкости обслуживаемой сети.

Серверное программное обеспечение, разработанное ООО «НТЦ ПРОТЕЙ», использует для своей работы следующее стороннее программное обеспечение, не входящее в заявляемый комплект: RedHat Linux или CentOS, возможны оба варианта.

Web-приложения, разработанные ООО «НТЦ ПРОТЕЙ», используют для своей работы следующее стороннее программное обеспечение, не входящее в заявляемый комплект: Apache Tomcat.

Хранение данных осуществляется с использованием СУБД Oracle.

Конкретная спецификация серверов (объём и количество винчестеров, мощность оборудования) обговаривается на этапе согласования технического задания согласно требованиям Заказчика.

Доступ на сервера для технического обслуживания модулей осуществляется по протоколам SSH.

На стадии поставки оборудования для всех Заказчиков логин и пароль одинаковы.

По просьбе Заказчика стандартные пароли могут быть заменены на уникальные.

Удаленный доступ на сервера с определенных адресов и портов Заказчик настраивает самостоятельно.

3.1 Требования к серверу

Для установки ПО необходимо аппаратное обеспечение (сервер) со следующими характеристиками:

Таблица 2. Характеристики сервера

№	Наименование характеристики	Значение

1.	Установка в шкаф 19 дюймов	Наличие
2.	Количество процессоров, штук	Не менее 2
3.	Количество ядер процессора, ядер	Не менее 6
4.	Тактовая частота процессора, ГГц	Не менее 2,2
5.	Объем оперативной памяти, Гб	Не менее 32
6.	Сетевой интерфейс 1 Гбит/с, штук	Не менее 4
7.	Количество жестких дисков, штук	Не менее 2
8.	Объем жесткого диска, Гб	Не менее 600
9.	Тип интерфейса жесткого диска	SAS
10.	RAID контроллер	Наличие

3.2 Требования к терминалу

Системный блок: частота процессора - не менее 1ГГц, объем оперативной памяти - не менее 2 Гб;

• монитор – 1 штука;

• клавиатура, мышь.

На терминале пользователя должна быть установлена операционная система и web-браузер.

К ОС предъявляются следующие требования:

- Linux: debian или red hat-системы с ядром linux версии 3.12 и выше;
- Windows версии 7 и выше;
- OS X версии El Capitan (10.11.4) и выше.

Требования к версиям поддерживаемых браузеров зависят от выбора ОС и представлены в таблице ниже.

Таблица 3. Требования к ОС и версиям браузера

ОС / Браузер	Linux	Windows	OS X
Firefox	38.0.1+	45.0.1+	46.0.1+
Chrome	43.0+	50.0+	50.0+
Chromium	50.0+	—	—
Safari	—	—	9.1+

3.3 Инструкция по установке

Предполагается, что на каждом сервере установлен Linux RedHat (или CentOS), винчестеры разбиты в соответствии с устанавливаемым на серверах ПО и настроена синхронизация времени.

Алгоритм установки:

1. Установить RPM-пакет protei-dpi-xxx.x86_64.rpm, где xxx — номер версии.
2. Выполнить прошивку плат DPI, выбор прошивки зависит от типа установленной платы. Для этого запустить файл: /usr/protei/Protei-DPI/utils/DPI_FirmwareUpdate_2.1.0.4.r. После указания сетевого интерфейса необходимо выбрать работу с Flash и типом User. После чего осуществить запись прошивки в память платы DPI (пункт Write firmware to flash).
3. Произвести настройку платы DPI, для этого необходимо запустить файл: /usr/protei/Protei-DPI/utils/DPI_FirmwareUpdate_2.1.0.4.r . После указания сетевого интерфейса необходимо выбрать пункт Write direction and vlans и произвести настройку платы DPI.
4. Установить RPM-пакет data-proc-xxx.noarch.rpm, где xxx — номер версии.
5. Распаковать архив apache-tomcat-8.0.21.tgz в директорию /usr/protei/OM.
6. Переместить файл WEB приложения DPI dpi.ui.apps.yyy.war в директорию /usr/protei/OM/apache-tomcat-xxx/webapps/ и переименовать его в DPI.war, где yyy — версия WEB приложения DPI, xxx- версия apache-tomcat (п.4).
7. Для установки СУБД Oracle необходимо распаковать архив

p13390677_112040_Linux-x86-64_1of7.zip в директорию /home/oracle/database, архив p13390677_112040_Linux-x86-64_2of7.zip в директорию /home/oracle/db-model. Затем установить RMP пакет oracle-rdbms-server-11gR2-preinstall-1.0-10.el6.x86_64.rpm.

8. Скачать следующие файлы в директорию /home/oracle/db-model: CreateDBCatalog.sql, Jserver.sql, lockAccount.sql, orcl.sql, README.txt, xdb_protocol.sql.
9. Установить СУБД Oracle /home/oracle/database/runInstaller -silent -showProgress -responseFile /home/oracle/db_11_ee.rsp, выполнить предложенные скрипты от пользователя с правами root.
10. От пользователя oracle запустить скрипт /home/oracle/db-model/orcl.sh, пароли установить как sql.
11. Для создания БД выполнить команду sqlplus и авторизоваться под пользователем SYSTEM, затем запустить скрипт: @orcl.sql.
12. Выполнить команду sqlplus и пройти авторизацию под пользователем SYSDBA, для создания табличного пространства и пользователей запустить скрипт: @create_tablespace_n_user.sql.
13. Выполнить команду sqlplus и пройти авторизацию под пользователем dpi_cdr, для создания схемы выполнить скрипт: @create_schema.sql.
14. Настроить автозапуск СУБД Oracle, для этого в файл /etc/oratab дописать следующую строчку (после этой строки обязательно нужен перевод строки): dpi_cdr:/usr/protei/data/oracle/OraHome.