Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК004.7: 004.057.4

Доля
Никита Анатольевич

Захват и анализ пакетного трафика

АВТОРЕФЕРАТ

на соискание степени магистра техники и технологии

по специальности 1-45 81 01 «Инфокоммуникационные системы и сети»

Научный руководитель

Астровский Иван Иванович
кандидат технических наук, доцент

Минск 2015

ВВЕДЕНИЕ

Анализ сетевого трафика приобретает все большую актуальность в связи с развитием и внедрением новых сетевых технологий (и, как следствие, увеличением объема данных, передаваемых по сети), а также появлением большого количества новых сетевых протоколов прикладного уровня. В качестве наиболее популярных областей практического применения захвата и анализа трафика можно выделить:

- учет использования сетевых ресурсов;
- администрирование трафика;
- обнаружение сетевых атак и вторжений;
- мониторинг качества сервиса (QoS).

Для организации коммуникаций в неоднородной сетевой среде применяется набор протоколов TCP/IP, обеспечивая совместимость между компьютерами разных типов. Совместимость – одно из основных преимуществ TCP/IP, поэтому большинство компьютерных сетей поддерживает эти протоколы. Кроме того, протоколы TCP/IP предоставляют доступ к ресурсам глобальной сети Интернет.

Среди существующих на сегодняшний деньподходов анализа трафика (стека протоколов TCP/IP)можно выделить следующие направления: на основе подготовленной заранее статистической модели,подходы с использованием методики допустимогопорога и отклонения характеристик и др. Все ониимеют свои плюсы и минусы.

В качестве мониторинга и анализа могут использоваться различные средства, как программно-аппаратные, так и программные. Компания CiscoSystems является крупнейшим производителем сетевого оборудования предлагает на рынке свое решение для анализа трафика – программно-аппаратный комплекс CiscoNAM 2304.

Целью магистерской диссертации является определение эффективных методов захвата и анализа трафика с помощью программно-аппаратного комплекса CiscoNAM 2304.

Достижение поставленной цели предполагает необходимость решения следующих задач:

- изучение стека протоколов TCP/IPи способ классификации IP-трафика;
- изучить технологии анализа трафика NetFlow, NBAR, SPAN;
- изучить программно-аппаратный анализатор трафика CiscoNAM 2304;
- разработать методику анализа трафика по технологии NetFlow, SPAN средствами CiscoNAM 2304;
- разработать методику определения пользовательского приложения с помощью анализатора трафика CiscoNAM2304.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Основной целью данной магистерской диссертации работы является определение методов захвата и анализа трафика, сравнение полученных результатов и предложение метода решения проблемы классификации неизвестного трафика в сети с помощью программно-аппаратного комплекса CiscoNAM 2304.

В первой главе рассмотрена архитектура семейства протоколов TCP/IP. IP-протокол является универсальным протоколом для любого типа приложений, используемых в компьютерных сетях, и вся нагрузка по транспорту трафиков ложится на него. Также известно, что основными транспортными протоколами, которые работают на IP, являются TCP и UDP. Сетевой трафик компьютерных сетей в основном состоит из TCP-трафиков, что является основной особенностью IP-трафика.

Во второй главе рассмотрены методы классификации IP-трафика. Классификация IP-трафика основывается на исследовании TCP и UDP номеров портов пакетов (классификация, основанная на портах), реконструкции сигнатуры протокола из его полезной нагрузки (классификация, основанная на полезной нагрузке), статистических методов анализа характеристик обмена пакетами между хостами и статистических свойств сетевого трафика. Каждый из подходов обладает своими достоинствами и недостатками.

В третьей главе проводиться обзор современных инструментов анализа сетевого трафика и их сравнительный анализ. Также описываются технологии для захвата и анализа трафика, которые могут применяться на сетевом оборудовании и использоваться в качестве источника информации о трафике для анализатораCiscoNAM 2304.

В четвертой главе разработаны методы захвата и анализа трафика с использованием программно-аппаратного комплекса CiscoNAM2304. Предложен метод с использованием технологии NetFlow иNBAR, а также метод с использованием функциональности анализатора коммутируемых портов (SPAN). Рассмотрен способ определения пользовательских приложений в CiscoNAM 2304. Проанализирована возможность оповещения о изменении относительно определенного порога заданной величины метрики трафика CiscoNAM 2304.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Исследования сетевых трафиков показали, что они представляют собой сложный динамический процесс и являются суперпозицией потоков с множественными взаимосвязанными характеристиками, которые генерируются различными протоколами.

Во-первых, этотрафики, связанные с управлением компьютерными сетями (например, трафик инициализации клиентов, серверный трафик и т.д.), которые генерируются периодически. Во-вторых, это трафики сетевых сервисов,приложений (например, DNS, FTP, запросы WINS, ARP, сеанс NetBIOS, HTTP, P2P, SMTP, POP3, Telnet и т.д.) и протоколов, которые составляют основную часть сетевого трафика компьютерных сетей.

IP-протокол является универсальным протоколом для любого типа приложений, используемых в компьютерных сетях, и вся нагрузка по транспорту трафиков ложится на него.

Также известно, что основными транспортными протоколами, которые работают на IP, являются TCP и UDP. Сетевой трафик компьютерных сетей в основном состоит из TCP-трафиков, что является основной особенностью IP-трафика. При этом, если рассмотреть более детально,структура сетевого трафика компьютерной сети состоит изIP-пакетов. Все трафики в компьютерных сетях, например, веб-трафики, трафики приложений, состоятиз серии IP-пакетов. Каждый IP-пакет состоит из заголовка и отправляемой информации. В свою очередь заголовок пакета состоит из полей с информацией об IP-адресе источника (отправителя), IP-адресе назначения (получателя), времени жизни пакета, типе сервиса, типе протокола, номере порта и т.д. При этом наиболее важными полями заголовка IP-пакета являются IP-адреса источника и назначения. Они используются для того, чтобы идентифицировать хосты отправителя и получателя. В компьютерных сетях каждый хост при соединении с другими хостами представляется уникальным идентификатором, состоящим из IP-адреса и номера порта. А на более высоком уровне агрегации имеются потоки IP-трафиков (веб-трафик, трафик приложений и т.д.), представляющие из себя наборы IP-пакетов с некоторыми одинаковымиключевыми атрибутами, например, IP-адреса источника и назначения, номер порта, тип протокола и т.д.

Классификация IP-трафика основывается на исследовании TCP и UDP номеров портов пакетов (классификация, основанная на портах), реконструкции сигнатуры протокола из его полезной нагрузки (классификация, основанная на полезной нагрузке), статистических методов анализа характеристик обмена пакетами между хостами и статистических свойств сетевого трафика.

В условиях постоянно растущего числа новых сетевых приложений наиболее эффективны методы классификации трафика на основе полезной нагрузки и на основе статистических методов, так как новые приложения могут использовать неизвестные порты взаимодействия по протоколу TCP/IP или скрываться за протоколами вышестоящих уровней, что требует глубокого анализа пакетов трафика.

Среди наиболее широко распространенных технологий анализа выделяются так называемые RBID-системы, основанные на правилах (Rule-BasedIntrusionDetection). Данные системы с целью выявления зловредного потока используют сравнение сигнатур с заранее подготовленной вирусной базой. После обнаружения атаки происходит анализ ее характеристик, а затем создается новое правило, которое в будущем обеспечит защиту от данного вида вторжения.

Другой подход к обнаружению информационных угроз имеют статистические системы (SBID). Статистический анализ относят к поведенческим методам определения неисправностей в компьютерных сетях. Данный подход основан на сопоставлении текущего состояния сети с определёнными заранее параметрами, описывающими правильное функционирование всей системы в целом.

Методы статистического анализа сетевого трафика используются в качестве инструментов прогнозирования загруженности каналов связи, диагностики искажений трафика, потерь информации и т.д., при этом они имеют различные интерпретации, основанные на различных характеристиках сетевого трафика. Главным преимуществом методов статистического анализа считается потенциальная возможность гарантировать безопасность не только от уже известных характеров атак, но и от предугаданных заранее.

Довольно крупную нишу занимает класс методов, основанных на маршрутизаторах. Важной составляющей данных методов является протокол простого сетевого мониторинга (SNMP). SNMP является частью протокола TCP/IP и позволяет осуществлять такие операции: сбор статистики по трафику, планирование роста сети, анализ производительности, обнаружение различных сетевых проблем и др. Для данного протокола существуют различные расширения, которые применяются в различных специфических отраслях. Среди них можно выделить удалённый мониторинг (RMON), который предоставляет возможность настраивать сигналы, диагностирующие сеть, основанные на определённом критерии, а также расширение Netflow, использующееся в маршрутизаторах Cisco, которое предоставляет возможность собирать IP сетевой трафик и преобразовывать данные для экспорта.

Распознавание сетевых приложений (англ. NetworkBasedApplicationRecognition, NBAR) — механизм, используемый в компьютерных сетях для распознавания потока данных (dataflow) по первому переданному пакету.

Оборудование компьютерных сетей, использующее NBAR производит тщательный анализ пакета (deeppacketinspection) для первого пакета в потоке данных для определения категории трафика, к которой принадлежит данный поток. Затем программное обеспечение настраивает внутренние ПЛИС для соответствующей обработки потока.

Средство NBAR представляет собой механизм классификации, который распознает широкий диапазон приложений, включая протоколы WWW и другие сложно квалифицируемые протоколы, использующие динамическое назначение портов TCP/UDP. После того как приложение определено и классифицировано с помощью средства NBAR, сеть может запускать службы для данного приложения. Средство NBAR обеспечивает эффективное использование полосы пропускания за счет классификации пакетов и использования функции QoS для классифицированного трафика.

Средство NBAR имеет новые методы классификации, позволяющие классифицировать приложения ипротоколы уровней с 3 по 7:

- Статическое назначение номеров портов TCP и UDP;
- IP-протоколы, не основанные на UDP и TCP;
- Динамическое назначение номеров портов TCP и UDP. Для классификации таких приложений необходима проверка сотслеживанием состояний, то есть способность обнаруживать подключения для передачи данных, которые необходимоклассифицировать, посредством анализа тех подключений, где выполнено назначение порта.
- Классификация подпортов или классификация на основе глубокой проверки пакетов, т.е. классификация с углубленным изучением пакета.

Задача анализа сетевого трафика приобретает все большую актуальность в

связи с развитием и внедрением новых сетевых технологий (и, как следствие, увеличением объема данных, передаваемых по сети), а также появлением большого количества новых сетевых протоколов прикладного уровня. В качестве наиболее популярных областей практического применения можно выделить:

- анализ трафика с целью выявления проблем в работе сети (в том числе, несанкционированной активности);
- восстановление потоков данных («прослушивание»);

– предотвращение различного рода сетевых атак;
– сбор статистики.

Система анализа должна обеспечивать захват 100% трафика, а также предоставлять эффективные методы анализа и навигации по его результатам.

CiscoNAM 2304 – программно-аппаратный комплекс мониторингаи анализа работы сети, которое объединяет анализ сетевого трафика на основе потоков и пакетов в единый набор инструментов. Cisco NAM выполняет функции анализатора протоколов,мониторинга состояния узлов сети, инструментария для управления качеством обслуживания (QoS), измерителя времени задержкии упреждающего мониторинга.

На основе проведенного исследования технологий захвата и анализа трафика были выработаны методы эффективного анализа трафика с помощью CiscoNAM 2304.

ЗАКЛЮЧЕНИЕ

В магистерской диссертации описана архитектура стека протоколовTCP/IP, структура пакетов популярных протоколов транспортного уровня. Рассмотрены методы классификации IP-трафика.Проанализированы возможности популярных программных и программно-аппаратных инструментов, дан их сравнительных анализ.

Для мониторинга и анализа пакетного трафика на удаленных узлах сети предлагается использовать технологию NetFlow. Данная технология позволяет получить информацию о потоке IP-трафика на уровнях L2-L4.Расширение возможности классификации трафика по приложениям достигается за счет использования совместно с технологией Netflowтехнологию глубокого анализа пакетов NBAR.

Разработана методика захвата и анализа трафика на базе программно-аппаратный комплекс CiscoNAM 2304 с использованием технологий NetFlowи NBAR. С помощью методики проведен анализ сетевого трафика в лабораторных условиях. CiscoNAM 2304 выступал в качестве коллектора и анализатора данных, полученных от сетевого оборудования по технологии NetFlow,что позволило классифицировать IP-трафика на L2-L7 уровнях.

Предложена методика захвата и анализа локального трафика по технологии SPAN средствами CiscoNAM 2304. Данная методика позволяет эффективно захватывать трафик для последующей его классификации на уровне приложений.

Для классификации пользовательских приложений предлагается использовать возможность определения нового приложения в классификаторе приложений CiscoNAM 2304. Добавление пользовательских приложений позволяет опционально определять новые приложения, что позволяет повысить эффективность классификации пакетного трафика.

Предложенные методики захвата и анализа трафика по технологиям NetFlow, NBARи SPAN могут найти применение в сферах:

- учет использования сетевых ресурсов;
- анализ трафика;
- администрирование трафика;
- обнаружение сетевых атак и вторжений;
- мониторинг качества сервиса (QoS).

Учет использования сетевых ресурсов основывается на NetFlowзаписях, которые обеспечивают точную информацию по принятому и переданному сетевому трафику конкретным пользователем сетевых ресурсов.

Согласно RFC 5472 учет использованных сетевых ресурсов может основываться на потоках между IP адресами или на классифицируемых

сервисах. В первом случае используются следующие информационные поляпакета NetFlow:

– IP адрес источника;

– IPадресприемника;

– тип используемого протокола;

– номера портов источника и приемника.

Во втором случае должны использоваться:

– точка кода дифференцированных услуг (DSCP);

– IP адреса источника и приемника.

Базовыми элементами, необходимыми для учета предоставленных сетевых ресурсов в обоих случаях являются количество переданных в потоке пакетов.

Анализ трафика подразумевает информацию, собранную предложенными методиками за большой период времени, которая может использоваться для отслеживания и прогнозирования роста сети и ее производительности. Это является необходимостью для анализа тенденций в сети и сетевом планировании. Параметры, которые представляют интерес, определяются конкретным объектом анализа. В качестве таких параметров можно указать: продолжительность потока, объем переданной в потоке информации, используемые протоколы и сервисы, количество пакетов определенного типа и другие.

Целью администрирования трафика является оптимизация сетевых ресурсов и параметров трафика. Типовыми параметрами являются:

– пропускная способность канала;

– загрузка между определенными сетями, узлами;

– число, размеры и точки входа/выхода активных потоков;

– маршрутизирующая информация.

Одним из применений предложенных методик захвата и анализа трафика является обнаружение сетевых атак и вторжений. В зависимости от типа атаки могут использоваться различные наборы метрик. Внезапное резкое возрастание трафика может служить одним из признаков начала атаки. CiscoNAM 2304 позволяет создать оповещение об отклонении величины метрики трафика от заданных нормальных статистических значений.

Мониторинг качества сервиса основывается на слежении за типовыми параметрами качества: потери, односторонняя и двусторонняя задержки (one-way и round-tripdelay), вариация задержки (delayvariation). Определение этих параметров требует обработки на уровне пакетов. Некоторые параметры качества сервиса требуют корреляции данных от нескольких точек наблюдения. Для этого необходима синхронизация по времени измерительных процессов в этих точках. Кроме этого необходимо распознавать, что один и тот же пакет

наблюдался в различных точках наблюдения. Это может быть сделано путем сбора частей содержимого пакета (заголовок пакета или части тела пакета), которые не изменялись на пути к приемнику. Основываясь на содержимом пакета, возможно определить, когда один и тот же пакет поступил в другую точку наблюдения. Для уменьшения количества измеряемых данных возможно вычисление уникального пакетного идентификатора на основе содержимого пакета.

Разработанные методики позволяют захватить и классифицировать трафик на уровне приложений средствами CiscoNAM 2304, что позволяет измерить параметры качества сети, качества голоса в IP-телефонии, параметры качества при взаимодействии пользователей с серверами.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

1. Доля Н.А. Захват и анализ сетевого трафика с помощью технологии SPANна базе сетевого анализатора CiscoNAM 2304 /Н.А. Доля, А.А. Антонович, А.В. Артамонов, О.Ю. Минченко, М.Д.А. Аль-Джебнаве // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы междунар. научно-технич. семинара. Минск, апрель-декабрь 2014 г. – Мн.: БГУИР, 2014. – С. 21-25.