УДК 654.1.02:004.357

ОЦЕНКА КАЧЕСТВА ПЕРЕДАЧИ ВИДЕОТРАФИКА В КОРПОРАТИВНОЙ СЕТИ

М.А. АЛИСЕЕНКО

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 22 октября 2018

Аннотация. Рассмотрены возможности применения систем захвата и анализа сетевого трафика для оценки качества передаваемого видеотрафика. Проведен обзор преимуществ технологий мониторинга и анализа трафика NetFlow и NBAR.

Ключевые слова: видеоконференцсвязь, анализ сетевого трафика, NetFlow, NBAR.

Введение

Для использования современных программных систем видеоконференцсвязи (ВКС) требуется только персональный компьютер (ПК) со встроенными внешними средствами отображения и воспроизведения данных. Программные системы ВКС предназначены для локальных корпоративных сетей, имеют программный MCU-сервер для управления участниками и видеоконференциями.

Наличие ВКС увеличивает объем передаваемых данных в сети, а также поддерживают большое количество сетевых протоколов прикладного уровня. Для разработки эффективной методики оценки качества передачи видеотрафика в корпоративной сети в условиях мультимедийного трафика требуется использовать системы анализа трафика.

Особенности систем захвата и анализа трафика

Выделяют следующие области практического применения систем анализа: выявление проблем в работе сети, восстановление («прослушивание») потоков данных, предотвращение сетевых атак, сбор статистики. Задача анализа сетевого трафика разделяется на три независимые подзадачи: перехват, хранение и анализ трафика. Система анализа должна обеспечивать захват трафика, а также предоставлять эффективные методы анализа его результатов.

Захват трафика осуществляется посредством снифферов – программ или программно-аппаратных устройств, предназначенных для перехвата трафика. В рамках конкретных продуктов могут быть реализованы дополнительные возможности, например, разбор заголовков сетевых протоколов, фильтрация по заданным критериям, восстановление сессий.

В сети Ethernet существуют следующие основные возможности прослушивания трафика [1].

1. В сети на основе концентраторов весь трафик домена коллизий доступен любой сетевой станции.

2. В сетях на основе коммутаторов сетевой станции доступен ее трафик, а также весь широковещательный трафик данного сегмента.

3. Управляемые коммутаторы имеют функцию копирования трафика данного порта на порт мониторинга («зеркалирование», мониторинг порта).

4. Допустимо использование специальных средств (ответвителей), включаемых в разрыв сетевого подключения и передающих трафик подключения на отдельный порт.

5. Порт коммутатора, трафик которого необходимо прослушать, включают через концентратор, к которому, в свою очередь, подключен узел-монитор (при этом в большинстве случаев уменьшается производительность сетевого подключения).

Сниффер может быть установлен на маршрутизаторе либо на оконечном узле сети.

Большинство существующих инструментов, как правило, проводит разбор заголовков сетевых протоколов, а также восстанавливает сессии. В то же время существуют достаточно специфические задачи, для решения которых может не отыскаться готовый инструмент [2]. К таким задачам относят:

– анализ туннелированных протоколов произвольной глубины;

– выделение связей между потоками данных, передаваемых по сети;

– выполнение определенных сценариев в случае обнаружения в трафике предварительно заданных сигнатур.

Выделяют два режима работы сетевых анализаторов: в реальном времени и по предварительно сохраненному трафику (отложенный анализ).

Для анализа в реальном времени требуется поддержка работы инструмента в непрерывном режиме с производительностью, достаточной для разбора трафика, поступающего на вход. При этом должна быть обеспечена возможность обработки потенциально бесконечного входного потока данных.

В случае отложенного анализа входные данные извлекаются из файла. Результаты такого анализа являются более детальными по сравнению с результатами анализа, выполняемого в режиме реального времени.

Технология NetFlow

В соответствии с NetFlow протоколом выполняется анализ пакетов, проходящих через определенный интерфейс сетевого устройства, на основе чего формируется информация в заданном формате о параметрах различных транзитных сетевых потоков интерфейса, и эта информация передается по IP сети специальной программе, называемой NetFlow коллектор. Программа NetFlow коллектор устанавливается на определенном ПК (сервере) сети и занимается сбором и первичной обработкой информации от одного или группы сетевых устройств, передающих данные в формате NetFlow. Затем используются программы, анализирующие накопленные данные и предоставляющие пользователю требуемые отчеты о работе сети.

Сетевой поток идентифицируется как однонаправленный поток пакетов между определенным источником и приемником данных, которые, в свою очередь, характеризуются IP-адресами и используемыми портами. Для уникальной идентификации потока используется 7 полей:

– IP адрес источника данных;

– IP адрес приемника данных;

– номер порта источника данных;

– номер порта приемника данных;

– тип протокола 3-го уровня;

– тип сервиса IP пакетов (ToS);

– входной логический интерфейс.

Существуют также программы-сенсоры NetFlow для компьютеров с различными операционными системами, которые позволяют формировать информацию о сетевых потоках, проходящих через интерфейсы ПК.

С помощью программного модуля на сетевом устройстве анализируются пакеты, проходящие через сетевой интерфейс, и на основании результатов анализа формируются данные по каждому сетевому потоку, проходящему через этот интерфейс в формате NetFlow протокола. Эти данные в виде отдельных записей по каждому сетевому потоку кэшируются. Каждая запись о потоке имеет уникальный идентификатор. Периодически данные из кэша пересылаются через сетевой интерфейс на ПК (сервер) с установленной программой NetFlow коллектор (см.рис. 1).

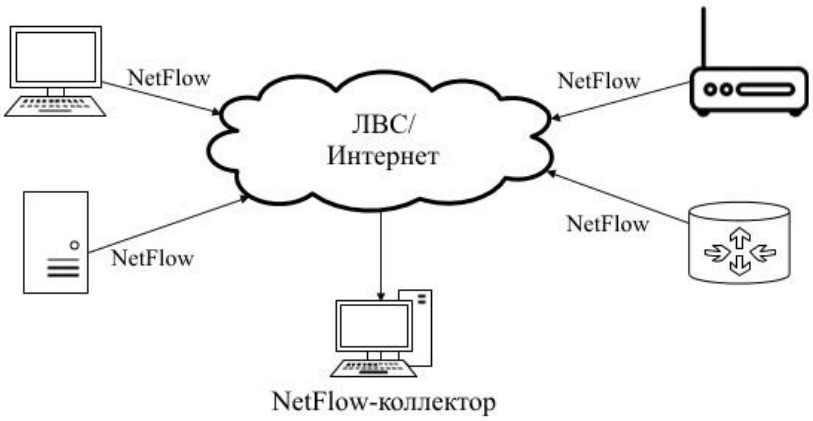

Рис. 1. Архитектура NetFlow

Таким образом, использование NetFlow протокола дополнительно загружает сетевой интерфейс, однако, благодаря высокой эффективности протокола, передаваемые данные занимают около 1,5 % от трафика коммутатора или маршрутизатора [3]. NetFlow протокол подсчитывает практически все пакеты и обеспечивает сжатый, но достаточно информативный обзор о всем сетевом трафике по интересующему сетевому интерфейсу.

Записи о сетевых потоках, которые утратили силу группируются в «NetF-low Export» дейтаграммы и экспортируются на сетевое устройство (ПК), с установленным NetFlow коллектором. Настройка NetFlow протокола выполняется для каждого интерфейса сетевого устройства. Для экспорта информации требуется указать IP адрес и номер порта устройства, где будет работать NetFlow коллектор.

Технология NBAR

Распознавание сетевых приложений Network Based Application Recognition (NBAR) − механизм, используемый в компьютерных сетях для распознавания потока данных по первому переданному пакету (рис. 2) [4].

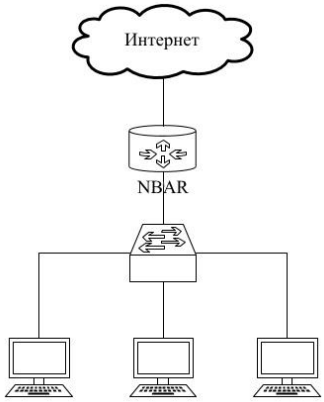

Рис. 2. Конфигурация NBAR

С помощью оборудования компьютерных сетей, использующего NBAR, анализ пакета для первого пакета в потоке данных для определения категории трафика, к которой принадлежит данный поток. Затем программное обеспечение настраивает внутренние контроллеры 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 и протоколы 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;

– Классификация подпортов или классификация на основе глубокой проверки пакетов.

В средстве NBAR предусмотрена возможность классификации протоколов статических портов. Несмотря на то, что для этих целей могут использоваться и списки управления доступом (access control list, ACL), настройка средства NBAR значительно проще. Кроме того, NBAR обеспечивает статистику по классификации, недоступную при использовании списков ACL.

В NBAR входит средство распознавания протоколов (Protocol Discovery), которое представляет собой простой способ поиска протоколов приложений, работающих через определенный интерфейс. Средство распознавания протоколов позволяет идентифицировать трафик любого протокола, поддержка которого реализована в средстве NBAR. По каждому протоколу средство распознавания протоколов выполняет сбор следующих статистических данных для активированных интерфейсов: полное число входящих и исходящих пакетов и байтов, а также входящая и исходящая скорость передачи данных. Средство распознавания протоколов собирает важнейшие статистические данные по каждому протоколу в сети, который может быть использован для определения классов трафика и политик QoS для каждого класса трафика. Для расширения списка распознаваемых протоколов может быть загружен внешний модуль языка описания пакета (PDLM). Модуль PDLM также используется для улучшения существующей способности распознавания. Модуль PDLM позволяет средству NBAR распознавать новые протоколы без необходимости в новых образах Cisco IOS или перезагрузке маршрутизатора.

Средство NBAR имеет возможность классифицировать трафик приложения не только по номерам портов TCP/UDP в пакете, но и классифицировать подпорты. Средство NBAR просматривает полезную нагрузку TCP/UDP и выполняет классификацию пакетов на основе содержимого полезной нагрузки, например, идентификатора транзакций, типа сообщений или других данных.

Классификация HTTP-трафика с помощью URL-адреса, узла сети или MIME-типа является примером классификации подпорта. NBAR классифицирует HTTP-трафик посредством текста URL или полей host в запросе, с применением поиска соответствий по регулярным выражениям. Реализованное в NBAR средство классификации типа полезной нагрузки RTP не только позволяет выполнять идентификацию аудио- и видеотрафика с отслеживанием состояния, но также позволяет осуществлять разграничения на основании типа аудио- и видеокодеков для повышения точности функции QoS. Таким образом, средство классификации типа полезной нагрузки RTP для классификации пакетов RTP осуществляет тщательное сканирование заголовков RTP.

Заключение

Таким образом, система анализа должна обеспечивать захват трафика в полном объеме, а также предоставлять эффективные методы анализа и навигации по его результатам. Технология мониторинга и анализа трафика NetFlow позволяет осуществлять мониторинг на уровнях L2-L4, идентифицировать приложения по номеру порта, предоставляет информацию о потоках IP пакетов. Технология глубокого анализа пакетов NBAR анализирует данные на уровнях L3-L7, обеспечивает комбинированный метод классификации IP-трафика на основе данных канального, сетевого и транспортного уровней, и анализе содержимого пакетов. Также NBAR идентифицирует видеотрафик и разграничивает нагрузку RTP для обеспечения QoS.

VIDEOTRAFFIC TRANSMISSION QUALITY ESTIMATION IN THE CORPORATE NETWORK

M.A. ALISEYENKA

Abstract. The possibilities of use of systems for capturing and analyzing network traffic to estimate the quality of transmitting videotraffic are considered. The benefits of monitoring and analyzing traffic NetFlow and NBAR technologies are reviewed.

Keywords: video conferencing, network traffic analysis, NetFlow, NBAR.

Список литературы

1. Национальный Открытый Университет «ИНТУИТ». [Электронный ресурс]. URL: https://www.intuit.ru/studies/courses/681/537. (дата обращения: 01.11.2018)
2. Маркин Ю.В., Санаров, А.С. // Обзор современных инструментов анализа сетевого трафика – Москва, 2014. С. 1–3.
3. Cisco NetFlow Collection Engine – Retirement Notification. [Электронный ресурс]. URL: http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/netflow/nfwhite.html. (дата обращения: 01.11.2018)
4. Хилл Б. Полный справочник по Cisco. М.: «Вильямс», 2007.