УДК 004.738.2

Константинов И.В., магистр,
2 курс, факультет «Отдел магистратуры»
Поволжского государственного университета телекоммуникаций и информатики
Россия, г. Самара
Фирсова А.А., магистр,
1 курс, факультет «Отдел магистратуры»
Поволжского государственного университета телекоммуникаций и информатики
Россия, г. Самара
Николаева А.В., студент,
4 курс, факультет «Базового телекоммуникационного образования»
Поволжского государственного университета телекоммуникаций и информатики
Россия, г. Самара
Научный руководитель: Васин Николай Николаевич

ИНСТРУМЕНТ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Аннотация: *В статье рассматривается инструмент анализа сетевого трафика. Рассмотрены различные аспекты анализа сетевого трафика, алгоритмы и подходы к анализу сетевого трафика, а также программно-аппаратные средства для эффективного решения этой задачи. В статье исследуется современное состояние этой области. Даны рекомендации, на что обратить внимание при использовании инструментов анализа сетевого трафика.*

Ключевые слова: *сетевой трафик, алгоритм, анализ, пакет, сеть.*

Annotation: *The article studies network traffic analysis tools. Various aspects of network traffic analysis are considered algorithms and approaches to network traffic analysis, as well as software and hardware tools for effectively solving this problem. The article studies the current state of this area. It is given recommendations on what to pay attention when using network traffic analysis tools.*

Key words: *network traffic, algorithm, analysis, packet, network.*

Сегодня анализ сетевого трафика — очень обширная тема. Под «анализом сетевого трафика» мы понимаем совокупное название технологий и их реализаций, позволяющих накапливать, обрабатывать, классифицировать, контролировать и модифицировать сетевые пакеты в зависимости от их содержания в режиме реального времени. Активное развитие сетевых технологий и расширение объема информационных услуг обеспечивают постоянный прирост новых пользователей, который носит ярко выраженный динамический характер. В то же время увеличивается объем сетевого трафика. Согласно исследованиям, примерная динамика роста трафика, передаваемого через всемирную паутину, составляет 70%-150% в год (за последние несколько лет), поэтому в среднем ежегодно объем передаваемой информации удваивается.

В более простом сегменте рынка можно найти анализаторы трафика, которые копируют проходящий трафик в файлы. Затем эту информацию необходимо обработать, чтобы получить точную картину моделей трафика. Также можно найти сложные системы, измеряющие трафик из нескольких точек сети одновременно. Они также могут комбинировать этот исходный материал для обнаружения необычного поведения пользователей.

Хотя сеть предоставляет данные в режиме реального времени, программ для анализа этого трафика в реальном времени очень мало. Заголовки пакетов являются основным источником информации для анализа, но анализаторы трафика ждут, пока серия пакетов не будет перехвачена и сохранена. Таким

образом, можно сказать, что анализ сетевого трафика работают на уровне приложений, а не на уровне сети.

Анализ сетевого трафика дает лучший обзор сетевой активности на уровне приложений. Информации, доступной на сетевом уровне, недостаточно для выявления общих шаблонов трафика, и она позволяет злонамеренному трафику намеренно распределяться по нескольким пакетам или агрегировать действия из разных источников.

Анализ сетевого трафика может дать быструю обратную связь, но в самом быстром режиме это «почти сделано». Приложения безопасности не могут обнаруживать угрозы, пока у них нет потоков данных для работы. При анализе возможностей меньше срочности, точность прогнозов важнее эффективности [1].

SolarWinds NetFlow Traffic Analyzer

Анализатор трафика SolarWinds NetFlow Рисунок 1 доступен как автономный монитор или как часть пакета анализатора пропускной способности сети, который также включает монитор производительности сети. Анализатор трафика NetFlow использует утилиты анализа пакетов, встроенные в сетевое оборудование, для получения образцов пакетов и показателей пропускной способности. Эти системы включают Cisco NetFlow, Juniper Networks J-Flow и Huawei NetStream, а также системы sFlow и IPFIX. Инструмент также интерпретирует данные NBAR2 с устройств Cisco.

Эти собранные данные можно просмотреть в режиме реального времени на экране. Утилита может обнаруживать VLAN (Virtual Local Area Network), например одновременный голосовой трафик на сеть. Функции данных в реальном времени включают пропускную способность потоков, которые предупредят вас, если трафик начнет превышать лимит пропускной способности вашей сети.

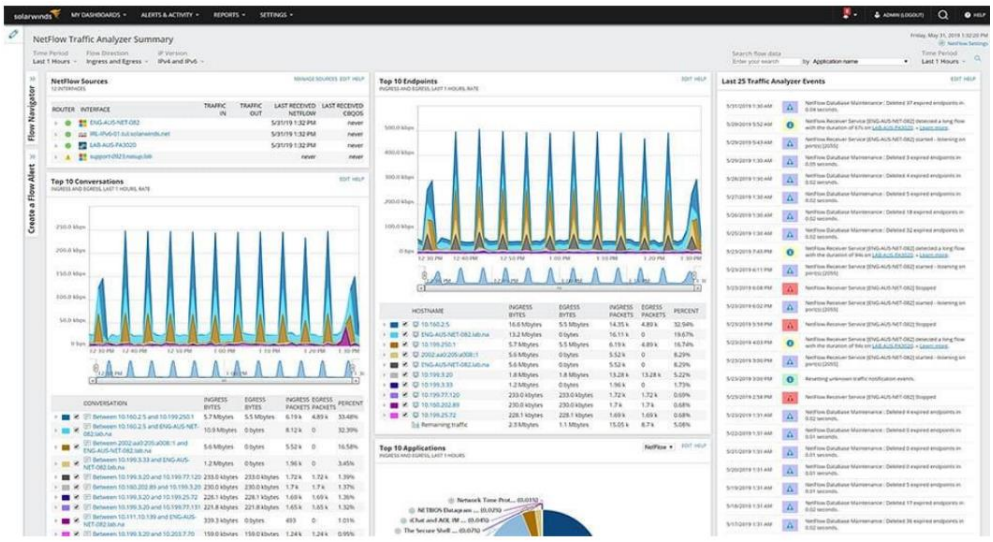

Рисунок 1. SolarWinds NetFlow Traffic Analyzer

На экранах анализа данных будут показаны приложения генерирует наибольшую часть трафика, а также может сегментировать данные по источнику и протоколу/порту. Диаграммы временной шкалы показывают пики трафика в течение часа, дней или месяцев. Это позволит вам оценить время пиковый спрос, чтобы вы могли перемещать пакетные задания и загрузки в менее важные часы.

Инструменты исправления в утилите включают формирование трафика меры, которые вы можете реализовать и управлять мерами формирования трафика на основе очередей, такими как QoS.

Программное обеспечение SolarWinds NetFlow Traffic Analyzer анализирует загрузки сети и полосы пропускания в режиме реального времени. Анализатор трафика SolarWinds NetFlow собирает данные из непрерывных потоков сетевого трафика и преобразует эти числа в простые для понимания графики и таблицы, которые точно показывают, как, кем и для какая корпоративная сеть используется.

Монитор производительности сети и NetFlow анализатор трафика может охватывать LAN, WLAN, WAN и подключаться к облачным сервисам. Оба эти инструменты устанавливаются на Windows Server и написаны на общей платформе, чтобы они могли взаимодействовать.

Ключевые особенности SolarWinds NetFlow Traffic Анализатор:

1. Инструменты анализа трафика. всеобъемлющий и гибкая панель инструментов позволяет получить полный обзор сетевого трафика на одной странице.
2. Поддержка оборудования от разных производителей. Анализатор трафика SolarWinds NetFlow анализирует NetFlow, J-Flow, sFlow, IPFIX и Huawei данные NetStream на устройствах от Cisco Systems, Extreme Networks, HP, Juniper, Nortel Networks и других ведущих производителей оборудования.
3. Анализ пропускной способности по приложениям. Передовой функции исследования приложений дают ценную информацию какие программы вызывают наибольшую пропускную способность потребление.
4. Уведомления, когда пропускная способность достигает потоков. Анализатор трафика SolarWinds NetFlow мгновенно оповещает администраторам, когда сетевой трафик превышает пропускную способность потоки. Уведомления содержат списки наиболее активных пользователей и приложений.

Вывод

В этой статье есть две основные причины для анализ сетевого трафика: улучшение сети проверки работоспособности и безопасность.

Программа SolarWinds NetFlow Traffic Analyzer является лучшией программой для проверки сетевого трафика. Оно работает с NetFlow, J-Flow, sFlow, NetStream и IPFIX для захвата пакетов.

Использованные источники:

1. Сниффинг сети на коммутаторах [Электронный ресурс]. URL: https://www.opennet.ru/base/sec/arp_snif.txt.html